



International Journal of Services, Economics and Management

ISSN online: 1753-0830 - ISSN print: 1753-0822
<https://www.inderscience.com/ijsem>

COVID-19 digital proximity-tracing applications: uptake, performance, and public health management implications

Izabella V. Lokshina, Cees J.M. Lanting

DOI: [10.1504/IJSEM.2026.10078749](https://doi.org/10.1504/IJSEM.2026.10078749)

Article History:

Received:	19 January 2026
Last revised:	25 March 2026
Accepted:	18 April 2026
Published online:	26 October 2026

COVID-19 digital proximity-tracing applications: uptake, performance, and public health management implications

Izabella V. Lokshina*

Department of Business,
SUNY Oneonta,
Oneonta, NY, 13820, USA
Email: izabella.lokshina@oneonta.edu
*Corresponding author

Cees J.M. Lanting

DATSA Belgium,
Leuven, VBR 3010, Belgium
Email: cees.lanting@datasaconsulting.com

Abstract: The COVID-19 pandemic profoundly disrupted public health systems worldwide, underscoring the need for tools to manage infectious disease transmission. Contact tracing has long been a core strategy in epidemic response, and the widespread availability of smartphones has enabled its evolution into digital proximity tracing via mobile applications. During the pandemic, numerous countries and regions implemented such apps based on location data and short-range communication technologies. This study examines the adoption, operational integration, and real-world effectiveness of digital proximity-tracing apps across multiple national contexts. Evidence suggests that these applications had a limited impact on reducing COVID-19 transmission due to low adoption rates and uneven integration into public health service operations. Furthermore, concerns about privacy, data security, and trust significantly influenced their adoption and performance. The findings emphasise that successful digital health interventions depend not only on technology but also on governance frameworks, communication strategies, and service design during public health emergencies.

Keywords: COVID-19; disease transmission; digital health interventions; contact tracing; digital proximity tracing; mobile applications; adoption; performance; concerns; privacy; data security; trust; public health management.

Reference to this paper should be made as follows: Lokshina, I.V. and Lanting, C.J.M. (2026) 'COVID-19 digital proximity-tracing applications: uptake, performance, and public health management implications', *Int. J. Services, Economics and Management*, Vol. 17, No. 5, pp.595–612.

Biographical notes: Izabella V. Lokshina has a PhD in Artificial Intelligence and is a Professor of Management Information Systems in the Department of Business at SUNY Oneonta. Her research is focused on emerging and state-of-the-art technologies.

Cees J.M. Lanting is a Senior Consultant at DATSA Belgium. His focus is on state-of-the-art technologies applied to system design and standardisation of IoT, health, and energy.

1 Introduction

This paper reviews a broad body of academic literature, government publications, and media reports to evaluate the development and deployment of digital proximity-tracing applications during the COVID-19 (SARS-CoV-2) pandemic. These applications were intended to identify individuals who had been in close contact, directly or indirectly, with infected or potentially infected persons, notify them of possible COVID-19 exposure, and encourage testing or self-isolation to reduce onward transmission.

As COVID-19 spread internationally in early 2020, governments began introducing digital proximity-tracing solutions, primarily during the spring of that year. These systems relied on either location-based tracking or short-range communication technologies to detect close encounters or interactions between infected individuals and others. Countries, regions, and subnational jurisdictions developed their own digital proximity-tracing applications, each operating within distinct legal, regulatory, and cultural environments.

Adoption rates varied widely. In some settings, digital proximity-tracing apps achieved prominent levels of use, while in others, uptake remained minimal. These outcomes were closely linked to public attitudes toward surveillance, institutional trust, and the strength of national governance frameworks (Johnson and Stewart, 2025; Lokshina and Lanting, 2023; Quach et al., 2025; Wang and Li, 2024).

The study first outlines the historical development of digital proximity tracing and the technologies underpinning it. Importantly, these tools did not rely on novel technological breakthroughs; instead, they repurposed existing smartphone and wireless communication capabilities (Danquah et al., 2019; Ferretti et al., 2020; Ha et al., 2013; Hu-Bolz et al., 2024; Kreps et al., 2020; Merry and Bettinger, 2019).

Subsequent sections examine global implementation strategies and report outcomes, drawing on existing research and emphasising factors that influenced effectiveness, including smartphone usage patterns, public confidence, and privacy and data security concerns.

From a technical standpoint, two primary models of digital proximity tracing emerged. The first is location-based tracing, which records an individual's presence at specific venues. The second relies on direct device-to-device communication to register proximity events when individuals remain within a defined distance for a specified duration.

Location-based systems log visits to places such as restaurants or public facilities, often assuming that accompanying individuals can be traced indirectly. While technically robust, this approach raises substantial privacy concerns given the collection of identifiable location data.

By contrast, person-to-person proximity tracing focuses on recording encounters that meet predefined time–distance thresholds. While this model can be implemented with robust privacy protection, its effectiveness has been inconsistent. Distance estimation errors are common due to variability in smartphone placement and the limitations of

Bluetooth hardware, which was not designed for precise distance measurement. Moreover, many prolonged proximity events occur among known contacts, limiting the added value of digital tracing for identifying unknown exposures. Specifically:

- Developers design digital proximity-tracing apps primarily to detect prolonged short-range interactions between individuals; however, imprecision in distance estimation generates significant errors in this domain.
- The location of a smartphone relative to the human body is too variable, introducing differences even when it is worn on or near the body.
- The Bluetooth subsystems of smartphones, including the antennas used, are not designed to measure distances accurately using Bluetooth signals, introducing phone-, subsystem-, position-, and direction-dependent variations.
- Proximity events, for instance, lasting 15 minutes at a short distance, mainly occur during meetings with other well-known people; such people are typically found in this individual's contact directory; therefore, the contribution to contact tracing is minimal.

Because these systems handle sensitive health-related information, compliance with fundamental privacy principles, such as informed consent, transparency, purpose limitation, proportionality, and security, is essential. At the same time, policymakers faced difficult trade-offs between protecting individual privacy and enabling effective public health surveillance during an emergency.

In general, potential misuse of private data, including its use by intelligence agencies, is a significant concern. While such invasive systems are typically unacceptable, a temporary increase in surveillance during a public health crisis may be tolerated as a trade-off between privacy and public health. This compromise aims to protect public health, healthcare infrastructure, businesses, and the broader economy (Johnson and Stewart, 2025; International Medical Informatics Association, 2011; Lokshina and Lanting, 2021; Nuffield Council on Bioethics, 2015; Pigera et al., 2025).

The primary aim of this paper is to evaluate the adoption and effectiveness of digital proximity-tracing applications across different countries. Drawing on existing research, it explores the technological, organisational, and governance determinants of success and failure, with particular attention to how public health authorities integrated these tools into established service-delivery systems.

Unlike prior studies that often focused on single-country experiences or purely technological aspects, this paper examines adoption, operational integration, and real-world effectiveness across multiple national contexts. By combining comparative analysis with governance, institutional, and social factors, this paper highlights conditions under which digital proximity-tracing apps are more effective. This broader perspective provides actionable insights into future public health interventions, clarifying why adoption, trust, privacy, and integration into existing public health workflows are critical to impact: insights that have not been fully captured in prior research.

This paper has several limitations that should be acknowledged:

- First, the analysis relies primarily on secondary sources, including scholarly publications, governmental reports, and media coverage, rather than original empirical data. As a result, findings depend on the accuracy, completeness, and

potential biases of existing documentation. Differences in reporting standards across countries may limit the comparability of outcomes.

- Second, measuring the effectiveness of digital proximity-tracing applications poses methodological challenges. Epidemiological impact is difficult to isolate from other public health interventions implemented simultaneously, such as lockdowns, vaccination campaigns, and manual contact tracing. Therefore, conclusions about the apps' independent effects should be interpreted cautiously.
- Third, the rapidly evolving nature of the COVID-19 pandemic means that policy environments, technological capabilities, and public attitudes shifted over time. This temporal variability may limit the generalisability of findings beyond the specific phases of the pandemic examined.
- Finally, contextual factors, including governance structures, levels of public trust, digital infrastructure, and legal frameworks, vary significantly across countries. While the paper identifies broad patterns, these findings may not be universally applicable to future public health emergencies or different sociopolitical contexts.

Despite these limitations, this paper provides a comparative and governance-focused perspective that contributes to understanding the conditional role of digital proximity tracing within broader public health strategies.

2 Digital proximity-tracing technologies

Early experiments with digital proximity tracing predate COVID-19 and were conducted primarily in regions facing high burdens of infectious diseases such as tuberculosis. In the early 2010s, pilot programs in countries such as Botswana showed the potential of mobile-based tracing systems, which were later replicated elsewhere in Africa. However, limited network infrastructure, particularly insufficient 3G bandwidth, severely restricted their effectiveness (Danquah et al., 2019; Ferretti et al., 2020; Ha et al., 2013; Kreps et al., 2020; Lokshina and Lanting, 2019; Merry and Bettinger, 2019; Nasereddin et al., 2023; Pozo-Martin et al., 2023).

Similar challenges occurred during the 2014–2016 Ebola outbreak in West Africa, where digital tracing efforts faced technical limitations and poor data collection. These experiences highlighted the importance of reliable infrastructure and user engagement (Danquah et al., 2019).

With the emergence of COVID-19, the widespread use of smartphones enabled the rapid scaling of digital proximity tracing. Most applications rely on Bluetooth technology, which is embedded in almost all modern smartphones (Apple.com, 2022; Centers for Disease Control and Prevention, 2020, 2022; Hu-Bolz et al., 2024; Ingram, 2020).

Under this model, devices exchange frequently changing, anonymous identifiers when they are within Bluetooth range for a defined period. If a user later tests positive and consents, their identifiers are uploaded to a server. Other devices periodically check these identifiers locally and notify users of potential exposure without revealing identities. Specifically, this model works to track COVID-19 as follows:

- Smartphones equipped with Bluetooth generate unique, anonymous codes that are exchanged between devices, enabling them to track close encounters without collecting personally identifiable information (PII).
- The proximity-tracing app generates these codes, which refresh every few minutes to preserve anonymity.
- When two phones with the app are within a given distance, e.g., ten feet within Bluetooth (Bluetooth LE) range (typically about 32 feet maximum) for a set period (as determined by health authorities to account for potential virus exposure), they exchange codes and store an encrypted record on each device.
- If someone tests positive for COVID-19, they can choose to share their result with a health agency, which then enters it into the app.
- The app then uploads the individual's anonymous data and codes to cloud servers.
- These servers distribute the codes to other phones, which then search for matching data. Individuals identified as having been in proximity to an infected person within the preceding 14 days are notified and advised to self-isolate, with anonymity preserved.

In response to widespread concerns about surveillance and potential misuse, Apple and Google jointly developed and released the Exposure Notification framework, embedding privacy protections at its core (Apple.com, 2022; Hu-Bolz et al., 2024; Johnson and Stewart, 2025). The system avoids location tracking, rotates identifiers frequently, processes data locally on devices, and requires explicit user consent for participation and data sharing. Specifically:

- The exposure notification Bluetooth specification uses only Bluetooth (Bluetooth LE) signals, not location data, to detect nearby devices.
- Each user's rolling proximity identifier updates every 15 minutes and must be paired with a temporary exposure key to establish any connection, helping protect user privacy by preventing tracking.
- All proximity identifiers collected from nearby devices are processed locally on the user's device.
- Participation in exposure notifications is entirely voluntary and under the control of the user.
- If a user tests positive for COVID-19, they must provide explicit consent before their Diagnosis Keys are sent to the server.
- The system provides users with complete transparency into how their data is used and their role in the exposure notification process.

Despite these safeguards, adoption rarely reached the targeted threshold, often cited as approximately 60% of the population, needed for optimal effectiveness. Decentralised architecture reduced privacy risks but limited public health authorities' ability to analyse population-level data (Bradford et al., 2020; Lokshina and Lanting, 2021; Pigera et al., 2025; UGA Today, 2020).

Bluetooth-based approaches were generally preferred over GPS-based systems, as GPS raises greater privacy concerns and performs poorly indoors (Ingram, 2020; Kreps et al., 2020; Merry and Bettinger, 2019). Because proximity detection relies on precise distance estimates, even small GPS errors can lead to considerable inaccuracies in identifying close contact or tracing proximity.

3 European experience with digital proximity tracing

Europe was among the first regions outside Asia to experience a severe COVID-19 outbreak, particularly in northern Italy in early 2020. Numerous European countries introduced proximity-tracing apps, but outcomes were mixed (Bradford et al., 2020; Juneau et al., 2023; Krämer et al., 2024; Lokshina and Lanting, 2021; Nasereddin et al., 2023; Quach et al., 2025).

Research examining Germany, Austria, and German-speaking Switzerland found that public discourse frequently framed these apps as instruments of surveillance. Interviews and media analysis revealed widespread ambivalence and distrust, even when apps were perceived as potentially useful.

According to research performed by Zimmerman et al. (2021), Germany, Austria, and Switzerland implemented proximity-tracing applications in 2020. The individuals interviewed by Zimmerman et al. (2021) were participants from the large Solidarity in Times of a Pandemic (SolPan) study, conducted in April 2020, which included people from 9 European countries. The SolPan study sought to collect people's experiences with policies and controls implemented by the various governments in the study to prevent the spread of the disease, such as movement restrictions, closures of workplaces and schools, and other measures.

Zimmerman et al. (2021) conducted qualitative interviews with 110 people from Germany, Austria, and German-speaking Switzerland who participated in the large SolPan study. Interviews, ranging from 25 to 80 minutes, covered their opinions on digital proximity-tracing applications and their use. The researchers found that both media coverage and the people interviewed described digital proximity-tracing applications as a form of government 'surveillance'. This term had different meanings for different people, including managing the spread of COVID-19 and consistently tracking people's movements.

However, such frequent use of this term, even when intended positively, suggested a general distrust and a lack of oversight associated with digital proximity-tracing apps. As a result, usage remained relatively low across these countries (Krämer et al., 2024; Zimmerman et al., 2021).

In Belgium, research showed moderate willingness to try proximity-tracing apps, driven primarily by the perceived benefit of receiving exposure notifications rather than fear of infection (Juneau et al., 2023; Walrave et al., 2020). Specifically, a survey of 730 Belgian people, conducted by Walrave et al. (2020), assessed acceptance of digital proximity-tracing applications. The results indicated a relatively high intent to try digital proximity tracing (about 49% of respondents), but not for the reasons one might expect.

Perceived severity of contracting COVID-19 and personal susceptibility to COVID-19 (in terms of having comorbidities such as diabetes or heart disease) were found not to influence the decision to use a digital proximity-tracing application.

Surprisingly, the most influential factor in this decision was the perceived benefit of being notified of proximity to individuals who had contracted COVID-19.

Therefore, respondents wanted information about their potential exposure, which drove their need for a digital proximity-tracing application. Another important reason for trying such an application was the need to adjust one's behaviour based on proximity to an infected person. This reasoning reflected a prosocial motivation: the desire to reduce the risk of infecting family members and friends by complying with quarantine or social distancing guidelines (Juneau et al., 2023; Walrave et al., 2020).

Similarly, studies in the Netherlands found that users valued data control and additional incentives, such as small financial rewards (Jonker et al., 2020; Krämer et al., 2024). Using a sample of 900 people from the Dutch population, Jonker et al. (2020) surveyed attitudes toward potential attributes of proximity-tracing apps.

Some interesting results regarding the potential use of such applications showed that potential users preferred features or benefits beyond merely tracking their proximity to COVID-19 infections. Small payments for using the application were cited as a popular desired attribute. Respondents also wanted to control their data as much as possible, given the nature of the application.

An interesting result of the survey was that most respondents preferred using an app with minimal proximity-tracing functionality rather than not using an app at all. Another result, which is not surprising, was that the predicted adoption rate for people under age 35 was higher than that for older people, especially those aged 75 years and older (Jonker et al., 2020; Krämer et al., 2024).

UK-based research highlighted concerns about privacy and government oversight, stressing the perceived need to balance individual rights with collective health benefits (Samuel et al., 2022). A digital proximity-tracing study conducted by Samuel et al. (2022) interviewed 35 participants from the UK who participated in the 2020 SolPan study cited earlier. Similar to studies in Germany, Austria, and German-speaking Switzerland, public discussion portrayed digital proximity-tracing apps as tools of surveillance, raising multiple issues related to data security, privacy, and government control. Notably, participants specifically mentioned the need to balance the privacy invasions caused by these apps with the societal benefits of proximity tracing.

Ireland stood out for comparatively higher acceptance, with most respondents indicating willingness to download a tracing app, motivated by a sense of social responsibility. Nonetheless, fears regarding government or corporate misuse of data persisted (Nasereddin et al., 2023; O'Callaghan et al., 2020).

The survey performed by O'Callaghan et al. (2020) in May 2020 yielded 8,088 responses from the Irish population about their attitudes toward digital proximity-tracing applications. The survey asked whether people would download a proximity-tracing app, and 54% said they would. Another 30% said they probably download an app.

The survey also asked respondents for the reasoning. Responses included the potential to help family and friends and a sense of responsibility to the broader community. These percentages and responses showed higher acceptance of digital proximity-tracing applications than in other countries. The survey also examined reasons for not downloading such an app; the most common response was fear of government or corporate misuse of data (Nasereddin et al., 2023; O'Callaghan et al., 2020).

Studies involving French health science students revealed low actual usage despite presumed higher awareness, reflecting broader trends of lower perceived risk among younger populations (Juneau et al., 2023; Montagni et al., 2020). The study conducted by

Montagni et al. (2020) examined the attitudes and practices of several hundred health science students toward the StopCovid application used in France.

It was logical to assume that health science university students owned mobile phones capable of using a digital proximity-tracing application. However, Montagni et al. (2020) found that only 11% of students were willing to download the app, and only 5% were using it at the time of the survey. This study was part of a larger effort to assess the health matters of the French student population. The results confirmed a global trend for lower perceived risk among younger populations (Juneau et al., 2023; Montagni et al., 2020).

Cross-national surveys revealed important levels of stated support for proximity tracing, while also highlighting considerable variation in trust, particularly concerning government surveillance (Altmann et al., 2020; Pigera et al., 2025; Pozo-Martin et al., 2023; Wang and Li, 2024).

A multi-country survey (France, Germany, Italy, the UK, and the USA) performed by Altmann et al. (2020) assessed support for digital proximity-tracing applications to sustain the COVID-19 mitigation efforts. In total, 5,995 responses were collected and analysed in March and April 2020. Consistent with research conducted in Ireland, these results showed that 4,484 participants (74.8%) reported having downloaded a digital proximity-tracing application used in their country.

The results confirmed that people who carried their mobile phones most of the day, for instance, working professionals and younger people, were more willing to download a digital proximity-tracing application. Additional results showed that people with comorbidities were 3.7% more willing to download an app. Specifically, this finding exposed a flaw in the digital proximity-tracing rollout strategy during the pandemic, highlighting the need to prioritise individuals with comorbidities before targeting the general population (Altmann et al., 2020).

Another finding showed that people in Germany and the USA were more concerned about the digital proximity-tracing app used for government surveillance. And, as in Ireland, support for the proximity-tracing app was driven by the desire to protect family and friends (Altmann et al., 2020; Pigera et al., 2025; Pozo-Martin et al., 2023).

4 North American context

Mobile health applications were already well established in North America before COVID-19. Nonetheless, digital proximity tracing encountered significant barriers in the USA due to political polarisation, fragmented governance, and privacy concerns (Bradford et al., 2020; Ha et al., 2013; Juneau et al., 2023; Krämer et al., 2024; Lokshina and Lanting, 2021; Nasereddin et al., 2023; Wang and Li, 2024).

Unlike many European countries, the USA implemented proximity tracing at the state level, resulting in uneven rollout and limited national coordination (MIT Technology Review, 2022; Nasereddin et al., 2023; National Academy for State Health Policy, 2022; Pennsylvania Department of Health, 2022). States pursued different development strategies, including in-house creation, interstate partnerships, and outsourcing to private vendors (Nasereddin et al., 2023; National Academy for State Health Policy, 2022).

While interoperability across state apps was often achieved, overall adoption remained low (MIT Technology Review, 2022; Quach et al., 2025). Download rates varied dramatically, ranging from minimal uptake in some states to moderate participation in others.

Modelling studies suggested that even modest adoption rates can reduce infections and fatalities when digital tracing complements manual contact tracing and social distancing (Abueg, 2020). However, real-world participation rarely approached optimal levels (Krämer et al., 2024; MIT Technology Review, 2022).

Canadian research focused more heavily on data governance and equity, raising concerns about surveillance, exclusion of populations without smartphones, and long-term impacts on public trust (McGrail, 2021). Similar issues emerged in Mexico and other parts of North America, where adoption remained extremely limited (ITSRIO, 2022; Kleinman and Merkel, 2020; MIT Technology Review, 2022; Pozo-Martin et al., 2023).

5 East Asian approaches

East Asia adopted more centralised and directive approaches to digital proximity tracing. China's Health Code system integrated location tracking into widely used platforms, assigning colour-coded risk statuses that determined access to public spaces (Mozur et al., 2020; Wang and Li, 2024; World Health Organization, 2020). Mandatory enforcement led to rapid and widespread adoption but raised concerns about long-term surveillance and data sharing with law enforcement (Mozur et al., 2020; Lokshina and Lanting, 2021; Nasereddin et al., 2023; Pozo-Martin et al., 2023; World Health Organization, 2020).

India's Aarogya Setu app combined Bluetooth and location tracking and was made mandatory for many citizens, resulting in the largest user base globally. Courts imposed restrictions on data retention and inter-agency sharing, reflecting ongoing privacy debates (Jalabneh et al., 2021; Plumber, 2021; Wang and Li, 2024).

Other countries, including Singapore, Malaysia, and Thailand, deployed a mix of Bluetooth-based and QR code systems. Singapore's TraceTogether app emphasised minimal data collection and automatic deletion, while Malaysia and Thailand implemented multiple apps with varying degrees of data access and privacy protection (Krämer et al., 2024; O'Neill et al., 2020; Pigera et al., 2025; Pozo-Martin et al., 2023; Wang and Li, 2024; Yuduang et al., 2022).

6 Latin and South America

Digital proximity tracing in Latin America faced structural and social barriers, including limited trust in government, economic inequality, and concerns over mobile data costs. Despite the rollout of numerous apps across the region, adoption and effectiveness varied (Boruchowicz et al., 2021; Privacy International, 2022; Wang and Li, 2024).

Countries such as Argentina and Uruguay achieved relatively high download numbers by integrating proximity tracing with symptom reporting and public information services (Scrollini and Baliosian, 2022). Elsewhere, multiple apps were launched with overlapping functions but limited coordination (Fox et al., 2021; Ordóñez and Ross, 2022; Wang and Li, 2024).

Overall, digital proximity tracing in the region struggled to overcome skepticism and infrastructural constraints (Fox et al., 2021; Nasereddin et al., 2023; Ordóñez and Ross, 2022; Pozo-Martin et al., 2023; Wang and Li, 2024).

7 Privacy, data security, and governance implications

Privacy and data protection emerged as central challenges worldwide (Bradford et al., 2020; Centers for Disease Control and Prevention, 2022; Johnson and Stewart, 2025; Pigera et al., 2025; Privacy International, 2022). Effective proximity tracing requires adherence to principles such as consent, transparency, proportionality, and security (International Medical Informatics Association, 2011; Nuffield Council on Bioethics, 2015). Yet centralised data storage, potential hacking, and misuse by state or non-state actors posed persistent risks (Lokshina and Lanting, 2021; Nasereddin et al., 2023; Pigera et al., 2025).

For instance, when digital proximity tracing was implemented to identify contacts of people who tested positive or were suspected of having the virus, a key strategy to contain the spread, it was important to uphold data privacy principles while establishing digital proximity-tracing apps as part of COVID-19 detection. Therefore, the main data privacy aspects must include consent, transparency, purpose limitation, proportionality, and security safeguards (Krämer et al., 2024; Lokshina and Lanting, 2021; Pigera et al., 2025).

According to Lokshina and Lanting (2021), the term ‘consent’ denotes agreeing to provide proximity-tracing data to designated collection points when required, comparable to signing official forms or employee declarations. The term ‘transparency’ explains how proximity-tracing data can be used. The term ‘purpose limitation’ indicates that personal information will be treated in strict confidence and used only to identify people to whom the virus may have spread. The term ‘security safeguards’ refers to measures taken to protect personal data from unnecessary sharing or leaks.

Implementing these measures would support secure proximity tracing and help maintain privacy and data security globally (Lokshina and Lanting, 2021). However, Lokshina and Lanting (2021) are concerned about data security issues, including the potential for private data to be exploited by malicious actors and stalkers.

Private data can be anonymised and encrypted, but these measures are insufficient to protect data stored in a centralised location and accessed remotely. Additionally, spoofed versions of digital proximity-tracing software may be distributed. For instance, agreements with Apple and Google could mitigate the issue but not eliminate it (Krämer et al., 2024; Lokshina and Lanting, 2021; Nasereddin et al., 2023; Pigera et al., 2025).

According to the current understanding, Lokshina and Lanting (2021) note that COVID-19 can be transmitted up to two weeks before symptoms appear and can spread through direct contact, surfaces, and the air. To protect privacy, it is essential not only to control access to contact data but also to limit how long it is stored. Contact information should be deleted after a recommended period, taking into account the virus’s incubation period and the delay in identifying potential exposure.

Additionally, there is a risk that private data could be repurposed for other uses, including by intelligence agencies. While such invasive digital proximity tracing would typically be deemed unacceptable, a temporary increase in surveillance may be tolerated as a necessary compromise between privacy and public health. This trade-off aims to protect public health, healthcare infrastructure, businesses, and the broader economy (Krämer et al., 2024; Lokshina and Lanting, 2021; Pigera et al., 2025).

Studies identified vulnerabilities in widely used APIs, including susceptibility to false exposure notifications and risks of deanonymisation through extended data retention (Baumgärtner et al., 2020; Biasin et al., 2022; Kamenjasevic and Biasin, 2020; Lokshina

and Lanting, 2023; Nasereddin et al., 2023; O'Neill et al., 2020; Pigera et al., 2025). Efforts to evaluate and rank apps based on privacy criteria revealed that only a minority met high standards of transparency and data minimisation (Krämer et al., 2024; MIT Technology Review, 2022).

For instance, the Centers for Disease Control and Prevention (CDC) in the USA classified digital proximity-tracing tools for COVID-19 into two categories: 'case management' and 'proximity tracing/exposure notification', based on how they assist in tracking and controlling the spread of COVID-19 (Centers for Disease Control and Prevention, 2022). These tools utilise smartphones or digital systems to identify individuals who may have been exposed to the virus and support public health efforts.

According to CDC (2022), public health departments use case management tools to monitor and manage infected cases and conduct contact-tracing investigations. People are alerted through proximity-tracing or exposure-notification tools when they are near someone infected, typically using smartphone apps. In both methods, technology plays a vital role in accelerating data collection and analysis, leading to faster and more effective communication of essential health information.

However, the use of technology also poses several challenges related to system security and user data privacy. Specifically, the CDC highlights two key disadvantages of digital proximity-tracing tools:

- Expanding the capabilities of the tool will require further consultation on the ethical and legal implications of electronic tracking; and
- Data security and confidentiality may be compromised by hacking or other unauthorised access or use (Centers for Disease Control and Prevention, 2020).

Indeed, research showed that some of the most widely used proximity-tracing application programming interfaces (APIs) developed by Google and Apple have security and privacy vulnerabilities. According to Baumgärtner et al. (2020), these APIs exhibit two significant vulnerabilities in their security and privacy safeguards.

First, Baumgärtner et al. (2020) uncovered a security flaw that could allow a malicious actor, using basic tools such as a mobile device or a Raspberry Pi, to carry out a 'wormhole attack'. This would enable the attacker to link two distant locations, making it appear as though a COVID-19 exposure in one area occurred in the other. As a result, individuals in the second location might receive false notifications, causing unnecessary panic among those who were not actually in proximity to an infected person.

Second, Baumgärtner et al. (2020) revealed a privacy concern involving the use of temporary exposure keys (TEKs). Both APIs rely on a 24-hour TEK, but some apps using these APIs request TEKs for multiple days, typically 14 days, based on the standard COVID-19 incubation period. Accumulating TEKs over a longer period increases the amount of data associated with an individual, thereby raising the risk of deanonymisation.

In May 2020, the MIT Technology Review began compiling a list of digital proximity-tracing apps launched worldwide and evaluating each app's privacy features (O'Neill et al., 2020). They established a set of key criteria, awarding a star for each criterion an app met. As outlined by O'Neill et al. (2020), these criteria include:

- Whether the app's use is voluntary.
- Whether there are limitations on how the data is used.

- Whether data is removed after a specified period, and whether data collection is minimised.
- Whether the process is transparent.

The database was last updated in March 2021, and 19 of 49 global apps earned a perfect five-star rating (MIT Technology Review, 2022).

Quantitative research supports the effectiveness of digital proximity-tracing applications in controlling the spread of COVID-19. These technology-based tools enable public health officials and individuals to respond more rapidly to potential COVID-19 exposures, allowing timely precautionary measures to prevent further transmission of the virus (Kamei et al., 2025).

For this reason, the continued use of these apps is advisable during a global pandemic. However, it is crucial to acknowledge and address the shortcomings of some of the most widely used APIs for these apps. This might raise an important question about how to enhance the security and privacy of digital proximity-tracing apps. The solution can lie in a combination of regulatory measures and technological improvements (Johnson and Stewart, 2025; Krämer et al., 2024; Lokshina and Lanting, 2023; Pigera et al., 2025).

Recent research suggests that digital proximity-tracing apps should be regulated and overseen by governments as medical devices (Kamenjasevic and Biasin, 2020). Biasin et al. (2022) demonstrate that these apps meet the criteria outlined in the European Union's MEDDEV guidelines for medical devices, addressing key classification questions, including:

- Does the product qualify as software under MEDDEV 2.1/6?
- Is the software considered standalone under the MEDDEV 2.1/6 definition?
- Does the software perform functions on data beyond storage, archiving, communication, or simple search?
- Is the software's action intended to benefit individual patients?

With affirmative responses to all key questions, Biasin et al. (2022) recommended treating and regulating digital proximity-tracing apps as medical devices. In addition to imposing stricter governmental oversight and regulation on the development and deployment of these apps, various technical solutions have been proposed to address existing security and privacy gaps.

Emerging proposals included regulating proximity-tracing apps as medical devices, adopting privacy-enhancing technical designs, and exploring blockchain-based solutions that allow users to retain control over their data (Ciaburro, 2022; Krämer et al., 2024; Lohan et al., 2022; Lokshina, 2022; Lokshina and Lanting, 2023; Mithani et al., 2022; Pigera et al., 2025).

One emerging proposal is the 'perturbed location' approach for digital proximity-tracing apps (Lohan et al., 2022; Pigera et al., 2025). According to Lohan et al. (2022), the model rests on two main assumptions: that users have full control over their location data and can access floor-map information when entering a building via a remote service provider.

The result is a digital proximity-tracing app that provides less granular location data, offering users greater privacy while still fulfilling the core functions of proximity tracing.

Although this solution would require additional development effort, such as mapping and collecting building floor plans, it offers potential not only for digital proximity-tracing apps but also for future location-based mobile apps that prioritise privacy over current models (Lohan et al., 2022).

Another widely researched approach is blockchain-based digital proximity-tracing solutions. Notably, several blockchain-based digital vaccine certificate applications have already been developed, supported by various organisations and companies, including major technology firms such as IBM (Mithani et al., 2022; Pozo-Martin et al., 2023).

Advocates for using blockchain in digital proximity tracing argue that it would provide greater security and privacy than current apps. With its user-centric data management model, blockchain allows individuals to retain ownership of their data (Ciaburro, 2022). Additionally, the immutable nature of blockchain ensures that once a block is added, it cannot be altered, providing a high level of reliability and transparency for all users (Ciaburro, 2022; Krämer et al., 2024; Lokshina, 2022).

Recent years have seen a strong drive to accelerate the development and deployment of digital proximity-tracing applications. As the virus persists, the need for robust proximity-tracing solutions remains critical. Contemporary research highlighted gaps in both technology and regulations, as well as potential solutions (Juneau et al., 2023; Kamei et al., 2025; Krämer et al., 2024; Lokshina, 2022; Lokshina and Lanting, 2023; Pigera et al., 2025).

Instead of settling for current systems, governments and technology developers should incorporate this research into the ongoing evolution of digital proximity tracing. These advancements could prove valuable not only for managing the COVID-19 pandemic but also for addressing future public health emergencies (Hu-Bolz et al., 2024; Kamei et al., 2025; Pigera et al., 2025).

8 Conclusions and recommendations

In this paper, the authors analysed a wide range of scholarly, governmental, and media sources to examine the adoption and effectiveness of COVID-19 digital proximity-tracing apps during the pandemic. Although many countries developed and deployed these applications as part of their public health response, effectiveness varied considerably across regions and public health service operations.

Unlike prior studies that mainly focused on single-country experiences or purely technological factors, this paper examined adoption, operational integration, and real-world effectiveness across multiple national contexts. This broader perspective provides practical insights for future public health efforts by emphasising why adoption, trust, privacy, and integration into existing public health systems are crucial for making an impact: insights that earlier research did not fully address.

This study showed that digital proximity-tracing apps played a limited but context-specific role in managing the COVID-19 pandemic. Adoption and effectiveness were highest in settings with strong centralised governance and clear directives, whereas decentralised and voluntary approaches often struggled to reach the participation levels needed for epidemiological impact.

Public trust, privacy protection, technological access, and institutional integration were decisive factors shaping outcomes. Without widespread adoption, digital proximity tracing offers only marginal benefits for controlling airborne infectious diseases.

Future public health emergencies may benefit from internationally coordinated platforms, potentially overseen by organisations such as the World Health Organization (WHO). However, such efforts must balance interoperability with respect for local governance, equity, and cultural context. For future public health emergencies, several targeted actions are recommended:

- Establish pre-approved legal and ethical frameworks that clearly define data use, storage limits, and deletion timelines before crises occur.
- Invest in public trust-building measures, including transparent governance structures, independent oversight, and proactive risk communication.
- Ensure interoperability standards to allow cross-border functionality, potentially coordinated by international bodies such as the WHO, while preserving national autonomy.
- Integrate digital tools directly into public health workflows, including testing, contact tracing teams, and case management systems, rather than deploying them as parallel or standalone systems.
- Address digital inequities by providing alternatives for individuals without smartphones and ensuring accessibility across age, income, and disability groups.
- Conduct ongoing evaluation and public reporting of effectiveness metrics to support accountability and adaptive improvement.

Ultimately, digital proximity tracing should be understood not as a standalone technological solution, but as one component of a broader public health strategy that integrates governance capacity, institutional coordination, social trust, and equitable service design. Its success depends less on technological advancement and more on alignment of digital infrastructure with public expectations, governance frameworks, and health system management.

Declarations

All authors declare that they have no conflicts of interest.

References

- Abueg, M., Hinch, R., Wu, N., Liu, L., Probert, W., Wu, A., Eastham, P., Shafi, Y., Rosencrantz, M., Dikovsky, M., Cheng, Z., Nurtay, A., Abeler-Dörner, L., Bonsall, D., McConnell, M. V., O'Banion, S. and Fraser, C. (2020) 'Modeling the combined effect of digital exposure notification and non-pharmaceutical interventions on the COVID-19 epidemic in Washington State', *medRxiv* 2020.08.29.20184135, DOI: 10.1101/2020.08.29.20184135.
- Altmann, S., Milsom, L., Zillesen, H., Blasone, R., Gerdon, F., Bach, R., Kreuter, F., Nosenzo, D., Toussaert, S. and Abeler, J. (2020) 'Acceptability of app-based contact tracing for COVID-19: cross-country survey study', *JMIR mHealth and uHealth*, Vol. 8, No. 8, p.e19857, DOI: 10.2196/19857, PMID: 32759102.
- Apple.com (2022) *Privacy-Preserving Contact Tracing*, Apple [online] <https://covid19.apple.com/contacttracing/> (accessed 31 May 2025).

- Baumgärtner, L., Dmitrienko, A., Freisleben, B., Gruler, A., Höchst, J., Kühlberg, J., Mezini, M., Mitev, R., Miettinen, M., Muhamedagic, A., Nguyen, T. D., Penning, A., Pustelnik, D., Roos, F., Sadeghi, A., Schwarz, M. and Uhl, C. (2020) 'Mind the GAP: security and privacy risks of contact tracing apps', *Proceedings of the 19th International Conference on Trust, Security and Privacy in Computing and Communications*, IEEE, pp.458–467, DOI: 10.1109/TrustCom50675.2020.00069.
- Biasin, E., Kamenjasevic, E. and Vedder, A. (2022) *Medical Device Software: A Use Case on Contact Tracing Apps*, Politecnico di Milano [online] <https://lirias.kuleuven.be/retrieve/663086> (accessed 12 April 2022).
- Boruchowicz, C., Boo, F.L., Roseth, B. and Tejerina, L. (2021) 'Default options: a powerful behavioural tool to increase COVID-19 contact tracing app acceptance in Latin America?', *Behavioural Public Policy*, Vol. 7, No. 3, pp.1–17, DOI: 10.1017/bpp.2021.38.
- Bradford, L., Aboy, M. and Liddell, K. (2020) 'COVID-19 contact tracing apps: a stress test for privacy, the GDPR and data protection regimes', *Journal of Law and Biosciences and Biosciences Special Issue: Law and Ethics in the Time of Global Pandemic*, Legal Studies Research Paper Series [online] <https://www.law.cam.ac.uk/ssrn> (accessed 30 April 2023).
- Centers for Disease Control and Prevention (2020) *Digital Contact Tracing Tools*, CDC [online] <https://www.cdc.gov/coronavirus/2019ncov/php/contact-tracing/contact-tracing-plan/digital-contact-tracing-tools.html> (accessed 12 April 2025).
- Centers for Disease Control and Prevention (2022) *Contact Tracing: Using Digital Tools*, CDC [online] <https://www.cdc.gov/coronavirus/2019-ncov/downloads/digital-contact-tracing.pdf> (accessed 12 April 2025).
- Ciaburro, G. (2022) 'Blockchain technology for contact tracing curing COVID-19', in Idrees, S.M. and Nowostawski, M. (Eds.): *Transformations Through Blockchain Technology*, pp.201–229, Springer, DOI: 10.1007/978-3-030-93344-9_9.
- Danquah, L.O., Hasham, N., MacFarlane, M., Conteh, F.E., Momoh, F., Tedesco, A.A., Jambai, A., Ross, D.A. and Weiss, H.A. (2019) 'Use of a mobile application for ebola contact tracing and monitoring in Northern Sierra Leone: a proof-of-concept study', *BMC Infectious Diseases*, Vol. 19, No. 1, p.810, DOI: 10.1186/s12879-019-4354-z PMID:31533659.
- Ferretti, L., Wymant, C., Kendall, M., Zhao, L., Nurtay, A., Abeler-Dörner, L., Parker, M., Bonsall, D. and Fraser, C. (2020) 'Quantifying SARS-CoV-2 transmission suggests epidemic control with digital contact tracing', *Science*, Vol. 638, No. 6491, p.eabb6936, DOI: 10.1126/science.abb6936 PMID:32234805.
- Fox, G., van der Werff, L., Rosati, P., Takako Endo, P. and Lynn, T. (2021) 'Examining the determinants of acceptance and use of mobile contact tracing applications in Brazil: an extended privacy calculus perspective', *Journal of the Association for Information Science and Technology*, Vol. 73, No. 7, pp.944–967, <https://doi.org/10.1002/asi.246021>.
- Ha, Y.P., Littman-Quinn, R., Antwi, C., Seropola, G., Green, R.S., Tesfalul, M. A., Ho-Foster, A., Luberti, A.A., Holmes, J.H., Steenhoff, A.P. and Kovarik, C.L. (2013) 'A mobile health approach to tuberculosis contact tracing in resource-limited settings', *Studies in Health Technology and Informatics*, Vol. 192, pp.1188–1188, DOI: 10.3233/978-1-61499-289-9-1188, PMID: 23920962.
- Hu-Bolz, J., Farrahi, K. and Cebrian, M. (2024) 'Beyond the surface of digital contact tracing: delving into the interconnected world of technology, individuals, and society', *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, Vol. 54, No. 10, pp.6332–6344.
- Ingram, D. (2020) *How Contact Tracing Could Use Bluetooth to Track Coronavirus on Your Smartphone*, NBC News, New York [online] <https://www.nbcnews.com/tech/tech-news/how-contact-tracing-could-use-bluetooth-track-coronavirus-your-smartphone-n1187796> (accessed 20 April 2020).
- International Medical Informatics Association (2011) *Code of Ethics for Health Information Professionals* [online] <http://www.imia-medinfo.org/new2/node/39> (accessed 12 April 2020).
- ITSRIO (2022) *Mexico's Covid Radar*, ITSRIO [online] <https://itsrio.org/wp-content/uploads/2020/07/COVIDRadar.pdf> (accessed 24 April 2025).

- Jalabneh, R., Syed, H.Z., Pillai, S., Apu, E.H., Hussein, M.R., Kabir, R., Arafat, S.M.Y., Majumder, M.A.A. and Saxena, S.K. (2021) 'Use of mobile phone apps for contact tracing to control the COVID-19 pandemic: a literature review', in Mohanty, S.N. et al. (Eds.): *Applications of Artificial Intelligence in COVID-19, Medical Virology: From Pathogenesis to Disease Control*, Springer, pp.389–404, DOI: 10.1007/978-981-15-7317-0_19.
- Johnson, D. and Stewart, A. (2025) 'Lifting information burdens to lifting lockdowns: administrative burden, citizen participation, and digital contact tracing', *Transforming Government: People, Process and Policy*, pp.1–21, <https://doi.org/10.1108/TG-08-2025-0243>.
- Jonker, M., de Bekker-Grob, E., Veldwijk, J., Goossens, L., Bour, S. and Rutten-Van Mölken, M. (2020) 'COVID-19 contact tracing apps: predicted uptake in the Netherlands based on a discrete choice experiment', *JMIR mHealth and uHealth*, Vol. 8, No. 10, p.e20741, DOI: 10.2196/20741 PMID:32795998.
- Juneau, C.E., Briand, A.S., Collazzo, P., Siebert, U. and Pueyo, T. (2023) 'Effective contact tracing for COVID-19: a systematic review', *Global Epidemiology*, December, Vol. 5, p.100103, DOI: 10.1016/j.gloepi.2023.100103, Epub 2023 Mar 9. PMID: 36959868; PMCID: PMC9997056.
- Kamei, Y., Tanabe, W., Ichikawa, M. and Okumura, T. (2025) 'Cross-national survey on the termination of digital contact tracing apps: have we killed the goose that lays the golden eggs?', *Informatics in Medicine Unlocked*, Vol. 59, p.101694, ISSN 2352-9148, <https://doi.org/10.1016/j.imu.2025.101694> [online] <https://www.sciencedirect.com/science/article/pii/S2352914825000838>.
- Kamenjasevic, E. and Biasin, E. (2020) 'Commentary on contact proximity tracing apps in the context of the EU legal framework for medical devices', *European Pharmaceutical Law Review*, Vol. 4, No. 2, pp.110–114, DOI: 10.21552/eplr/2020/2/8.
- Kleinman, R.A. and Merkel, C. (2020) 'Digital contact tracing for COVID-19', *Canadian Medical Association Journal*, Vol. 192, No. 24, pp.E653–E656, <https://doi-org.ezaccess.libraries.psu.edu/10.1503/cmaj.200922>.
- Krämer, D., Brachem, E., Schneider-Reuter, L., D'Angelo, I., Vollmann, J. and Haltaufderheide, J. (2024) 'The role of transparency in digital contact tracing during COVID-19: insights from an expert survey', *Health Care Analysis*, <https://doi.org/10.1007/s10728-024-00485-z>.
- Kreps, S., Zhang, B. and McMurry, N. (2020) *Contact Tracing Apps Face Serious Adoption Obstacles*, Brookings Institution Tech Stream [online] <https://www.brookings.edu/techstream/contact-tracing-apps-face-serious-adoption-obstacles/> (accessed 12 April 2020).
- Lohan, E.S., Shubina, V. and Dragos, N. (2022) 'Perturbed-location mechanism for increased user-location privacy in proximity detection and digital contact tracing applications', *Sensors*, Vol. 22, No. 687, p.687, DOI: 10.3390/s22020687, PMID: 35062648.
- Lokshina, I. (2022) 'Revisiting state-of-the-art applications of blockchain technology in business ecosystems: analysis of open issues and potential solutions', *International Journal of Interdisciplinary Telecommunications and Networking*, Vol. 14, No. 1, pp.1–21, DOI: 10.4018/IJITN.299370.
- Lokshina, I. and Lanting, C. (2019) 'A qualitative evaluation of IoT-driven ehealth: knowledge management, business models and opportunities, deployment and evolution', in Kryvinska, N. and Greguš, M. (Eds.): *Data-Centric Business and Applications, Lecture Notes on Data Engineering and Communications Technologies*, Vol. 20, Springer, Cham, https://doi.org/10.1007/978-3-319-94117-2_2.
- Lokshina, I. and Lanting, C. (2021) 'Study on wide-ranging ethical implications of big data technology in a digital society: how likely are data accidents during COVID-19?', *Journal of Business Ecosystems*, Vol. 2, No. 1, pp.32–57, DOI: 10.4018/JBE.2021010103.
- Lokshina, I. and Lanting, C. (2023) 'Evolution of public health data regulatory models from a linked democracy perspective', *New Trends in Computer Sciences*, Vol. 1, No. 2, pp.70–96, DOI: <https://doi.org/10.3846/ntcs.2023.19166>.

- McGrail, K.M. (2021) 'Contact tracing apps: time to confront broader societal change', *American Journal of Public Health*, Vol. 111, No. 3, pp.369–370, DOI: 10.2105/AJPH.2020.306084 PMID:33566643 [online] <https://ezaccess.libraries.psu.edu/login?url=https://www.proquest.com/scholarly-journals/contact-tracing-apps-time-confront-broader/docview/2516963488/se-2?accountid=13158> (accessed 12 April 2022).
- Merry, K. and Bettinger, P. (2019) 'Smartphone GPS accuracy study in an urban environment', *PLOS ONE* [online] <https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0219890> (accessed 12 April 2020).
- MIT Technology Review (2022) *We Investigated Whether Digital Contact Tracing Actually Worked in the US*, MIT [online] <https://www.technologyreview.com/2021/06/16/1026255/us-digital-contact-tracing-exposure-notification-analysis> (accessed 12 April 2025).
- Mithani, S.S., Bota, A.B., Zhu, D.T. and Wilson, K. (2022) 'A scoping review of global vaccine certificate solutions for COVID-19', *Human Vaccines and Immunotherapeutics*, Vol. 18, No. 1, pp.1–12, DOI: 10.1080/21645515.2021.1969849, PMID: 34613869.
- Montagni, I., Roussel, N., Thiebaut, R. and Tzourio, C. (2020) 'The French COVID-19 contact tracing app: usage and opinions by students in the health domain', *medRxiv* 2020.10.23.20218214, DOI: 10.1101/2020.10.23.20218214.
- Mozur, P., Zhong, R. and Krolik, A. (2020) 'In the coronavirus fight, China gives citizens a color code, with red flags', *The New York Times* [online] <https://www.nytimes.com/2020/03/01/business/china-coronavirus-surveillance.html> (accessed 12 April 2020).
- Nasereddin, M., Bartolacci, M., Peca, J.C., Glantz, E.J., Grimes, G. and Verlati, T. (2023) 'Digital contact tracing for COVID-19: a review of its application to the global pandemic', *International Journal of Disaster Response and Emergency Management*, Vol. 6, No. 1, pp.1–16, <https://doi.org/10.4018/IJDREM.324084>.
- National Academy for State Health Policy (2022) *State Approaches to Contact Tracing COVID-19*, NASHP [online] <https://www.nashp.org/state-approaches-to-contact-tracing-covid-19/> (accessed 12 April 2025).
- Nuffield Council on Bioethics (2015) *The Collection, Linking, and Use of Data in Biomedical Research and Healthcare: Ethical Issues*, The Nuffield Council on Bioethics, London [online] http://nuffieldbioethics.org/wp-content/uploads/Biological_and_health_data_web.pdf (accessed 12 April 2020).
- O'Callaghan, M.E., Buckley, J., Fitzgerald, B., Johnson, K., Laffey, J., McNicholas, B., Nuseibeh, B., O'Keeffe, D., O'Keeffe, I., Razzaq, A., Rekanar, K., Richardson, I., Simpkin, A., Abedin, J., Storni, C., Tsvyatkova, D., Walsh, J., Welsh, T. and Glynn, L. (2020) 'A national survey of attitudes to COVID-19 digital contact tracing in the Republic of Ireland', *Irish Journal of Medical Science*, Vol. 190, No. 3, pp.863–887, DOI: 10.1007/s11845-020-02389-y, PMID: 33063226.
- O'Neill, P.H., Ryan-Mosley, T. and Johnson, B. (2020) 'A flood of coronavirus apps is tracking us. Now it is time to keep track of them', *MIT Technology Review* [online] <https://www.technologyreview.com/2020/05/07/1000961/launching-mitr-covid-tracing-tracker/on/5/5/22> (accessed 12 April 2025).
- Ordóñez, S. and Ross, G. (2022) *Tracing Latin America's Contact Tracing*, Wilson Center [online] <https://www.wilsoncenter.org/blogpost/tracing-latin-americas-contact-tracing> (accessed 12 April 2025).
- Pennsylvania Department of Health (2022) *Coronavirus*, PDH [online] <https://www.health.pa.gov/topics/disease/coronavirus/Pages/COVIDAlert.aspx> (accessed 12 April 2025).
- Pigera, S., Van Schaik, P., Renaud, K., Campbell, M., Manley, P. and Esser, P. (2025) 'Privacy and security in digital health contact tracing: a narrative review', *Applied Sciences*, Vol. 15, No. 2, p.865.
- Plumber, M. (2021) 'No informed consent: karnataka high court restrains centre and NIC from sharing response data of persons collected through Aarogya Setu', *Live Law* [online] <https://www.livelaw.in/top-stories/karnataka-high-court-restrains-centre-nic-from-sharing-response-data-of-persons-collected-through-aarogya-setu-168886> (accessed 25 January 2021).

- Pozo-Martin, F., Beltran Sanchez, M.A., Müller, S.A., Diaconu, V., Weil, K. and El Bcheraoui, C. (2023) 'Comparative effectiveness of contact tracing interventions in the context of the COVID-19 pandemic: a systematic review', *European Journal of Epidemiology*, Vol. 38, No. 3, pp.243–266.
- Privacy International (2022) *Argentina Requires App Monitoring for Incoming Travellers' Quarantine*, PI [online] <https://privacyinternational.org/examples/3567/argentina-requires-app-monitoring-during-incoming-travellers-quarantine> (accessed 1 April 2020).
- Quach, H.L., Walsh, E.I., Hoang, T.N.A., Terrett, R.N.L. and Vogt, F. (2025) 'Effectiveness of digital contact tracing interventions for COVID-19: a systematic scoping review', *Public Health*, May, Vol. 242, pp.146–156, DOI: 10.1016/j.puhe.2025.02.019, PMID: 40068321.
- Samuel, G., Roberts, S.L., Fiske, A., Lucivero, F., McLennan, S. A., Phillips, A., Hayes, S. and Johnson, S.B. (2022) 'COVID-19 contact tracing apps: UK public perceptions', *Critical Public Health*, Vol. 32, No. 1, pp.31–43, DOI: 10.1080/09581596.2021.1909707, PMID: 35221546.
- Scrollini, F. and Baliosian, J. (2022) 'Uruguay's COVID-19 contact tracing app reveals the growing importance of data governance frameworks', *LSE Blogs* [online] <https://blogs.lse.ac.uk/latamcaribbean/2020/08/26/uruguays-covid-19-contact-tracing-app-reveals-the-growing-importance-of-data-governance-frameworks/> (accessed 22 May 2022).
- UGA Today (2020) 'Smartphone GPS accuracy may affect contact tracing', *UGA Today* [online] <https://news.uga.edu/smartphone-gps-accuracy-affect-contact-tracing> (accessed 22 May 2022).
- Walrave, M., Waeterloos, C. and Ponnet, K. (2020) 'Adoption of a contact tracing app for containing COVID-19: a health belief model approach', *JMIR Public Health and Surveillance*, Vol. 6, No. 3, p.e20572, DOI: 10.2196/20572, PMID: 32755882.
- Wang, J. and Li, Y. (2024) 'Digital contact tracing for pandemic response: the roles of cultural worldviews and technology awareness', *Information Systems Research*, Vol. 35, No. 4, pp.1766–1784.
- World Health Organization (2020) *COVID-19 – China*, WHO [online] <https://www.who.int/emergencies/disease-outbreak-news/item/2020-DON229> (accessed 5 January 2025).
- Yuduang, N., Ong, A.K.S., Prasetyo, Y.T., Chuenyindee, T., Kusonwattana, P., Limpasart, W., Sittiwatethanasiri, T., Gumasing, M.J.J., German, J.D. and Nadlifatin, R. (2022) 'Factors influencing the perceived effectiveness of the COVID-19 risk assessment mobile application 'Morchana' in Thailand: Utaut2 approach', *International Journal of Environmental Research and Public Health*, Vol. 19, No. 9, p.5643, DOI: 10.3390/ijerph19095643, PMID: 35565040.
- Zimmermann, B.M., Fiske, A., Prainsack, B., Hangel, N., McLennan, S. and Buyx, A. (2021) 'Early perceptions of COVID-19 contact tracing apps in German-speaking countries: comparative mixed methods study', *Journal of Medical Internet Research*, Vol. 23, No. 2, p.e25525, DOI: 10.2196/25525 PMID:33503000.