The Turkish Online Journal of Design, Art and Communication

E-ISSN: 2146-5193

DOI: 10.7456/tojdac

Research Article / Araştırma Makalesi

CONCERNS OF THE PEOPLE IN TURKEY REGARDING THE NATIONAL CONTACT TRACING MOBILE APPLICATION OF THE COVID-19 PERIOD

TÜRKİYE'DE BİREYLERİN COVID-19 DÖNEMİNDE KULLANILAN ULUSAL TEMAS TAKİP UYGULAMASINA İLİŞKİN ENDİŞELERİ

Ü. Laçin YALÇINKAYA[1]
Cem S. SÜTCÜ[2]
İhsan EKEN[3]

ORCID: U.L.Y. 0000-0002-7372-8700
C.S.S. 0000-0002-9389-6832
I.E. 0000-0002-0401-8545

Corresponding author/Sorumlu yazar:
[1] Ü. Laçin Yalçınkaya
Istanbul Medipol University, Türkiye
E-mail/E-posta: umit.yalcinkaya@medipol.edu.tr

[2] Cem S. Sütcü
Marmara University, Türkiye
E-mail/E-posta: csutcu@marmara.edu.tr

[3] İhsan Eken
Istanbul Medipol University, Türkiye
E-mail/E-posta: ieken@medipol.edu.tr

Received/Geliş tarihi: 25.04.2024

Benzerlik Oranı/Similarity Ratio: %3

Revision Requested/Revizyon talebi: 20.05.2024

Last revision received/Son revizyon teslimi: 30.05.2024

Accepted/Kabul tarihi: 31.05.2024

Etik Kurul İzni/ Ethics Committee Permission: İstanbul Medipol University, Ethical Committee for Scientific Research in Social Sciences / Issue Number: 54 / 22/04/2024

Citation/Atıf: Yalcinkaya, U. L., Sutcu, C. S. & Eken, I. (2024). Concerns of the People in Turkey Regarding the National Contact Tracing Mobile Application of the COVID-19 Period. The Turkish Online Journal of Design Art and Communication, 14 (3), 735-752. https://doi.org/10.7456/tojdac.1473413.

Abstract
Contact tracing mobile applications (CTMAs) were used by many governments worldwide within their COVID-19 response strategies. They were also being debated widely since they pose risks regarding personal data privacy. The Republic of Turkey Ministry of Health deployed a CTMA called the HES app, to complement the manual contact tracing efforts. However, since its release, it has garnered significant criticism from experts advocating data privacy and human rights. By reviewing the available literature, we designed a quantitative research to explore if the individuals living in Turkey also have the concerns expressed by the experts regarding the HES application. Due to lockdown measures, we collected the data through an online survey, which we developed based on the main points of concern voiced globally about the concept of CTMA from 457 participants who gave informed consent. According to our findings, worries regarding the HES application do exist and are prevalent among individuals living in Turkey, independent of their socio-economic status. The concerns can be grouped under two main categories, namely, having concerns about invasive digital surveillance, and the lack of belief in the legitimacy of the HES application. Therefore, we suggest that the application's architecture be reorganized in a decentralized, transparent, auditable, privacy-preserving manner for future health crises to better serve public health.

Keywords: Contact tracing mobile applications, digital surveillance, data privacy, COVID-19.

Öz
Temas takip uygulamaları, COVID-19 salgınıyla mücadele amacıyla dünyanın birçok ülkesinde kullanılmıştır. Ancak bu uygulamaların meşruiyeti, veri mahremiyeti adına taşıdıkları riskler sebebiyle, geniş çevrelerce tartışılmıştır. Söz konusu dönemde, Türkiye Cumhuriyeti Sağlık Bakanlığı da Hayat Eve Sığar (HES) adlı uygulamayı kullanıma sunmuştur. Ancak uygulama, veri gizliliği ve insan hakları alanlarında çalışan uzmanlardan yaygın şekilde eleştiri toplamıştır. Çalışma kapsamında, uzmanlar tarafından dile getirilen endişelerin, uygulamanın kullanıcıları tarafından taşınıp taşınmadıklarının anlaşılması amacıyla nicel bir araştırma tasarlanmıştır. Araştırmanın verisi; gönüllü onam vermiş 457 katılımcıdan, temas takip uygulamalarına ilişkin dünya çapında dile getirilen endişelerden hareketle yapılandırılmış bir ölçek kullanılarak - dönemin karantina koşulları uyarınca - çevrimiçi şekilde toplanmıştır. Bulgularımız Türkiye'de yaşayan bireylerin, sosyoekonomik durumlarından bağımsız olarak, HES uygulamasına ilişkin endişeler taşıdıklarını göstermektedir. Söz konusu endişeler artan dijital gözetim korkusu ve HES uygulamasının meşruluğuna duyulan güvensizlik olmak üzere iki ana kategori altında toplanmaktadır. Sonuçlardan hareketle, gelecekte karşılaşılabilecek sağlık krizlerinde temas takip uygulamalarından alınan faydanın artırılabilmesi için; uygulama mimarisinin bireylerin veri mahretmiyetine saygılı, merkezi olmayan, şeffaf ve denetlenebilir bir yapıda yeniden düzenlenmesini öneriyoruz.

Anahtar Kelimeler: Temas Takip Uygulamaları, Dijital Gözetim, Veri Mahremiyeti, COVID-19.

INTRODUCTION

During the COVID-19 pandemic, measures taken by the public health authorities (PHAs) to control the spread of the virus may have been seen as the most crucial part of fighting the disease. Considering the high contagiousness of the virus, the PHAs placed utmost importance on utilizing nonpharmaceutical measures, such as case isolation, household quarantine, closure of schools and workplaces, and travel restrictions (Ekong et al., 2020).

In the event of a pandemic, it is widely accepted that indiscriminate lockdowns can cause severe economic consequences (Loayza, 2020; Whitelaw et al., 2020). Thus, discriminatory measures, such as mandatory self-isolation applied only to the infected individuals to prevent them from spreading the virus further, are highly important. This is where the dilemma comes into play: Several studies presented evidence that asymptomatic and presymptomatic transmission played a significant part in the rapid spread of COVID-19 (Ferretti et al., 2020; Gandhi et al., 2020; Oran & Topol, 2020). Then, the question is: How can the potential virus spreaders be determined and be demanded to self-isolate if they do not show any symptoms? Considering the scarcity of test kits in the early phases of the pandemic (Cho et al., 2020; Ekong et al., 2020), this very question made the contact tracing efforts, whether the traced individual is confirmed to be infected or not, into a critical component of containing the disease.

Known as a well-accepted disease control practice (Clarke, 1998; Donnelly et al., 2003), contact tracing is a form of disease surveillance mainly focusing on determining potential new cases (Eames & Keeling, 2003). According to the World Health Organization (WHO), it breaks the chains of interpersonal transmission by identifying the individuals who had contact with confirmed cases, quarantining them, following them up to ensure timely isolation, and proceeding with testing and treatment if necessary (2020a). Thanks to the digital capacity built by the network society (see Dijk, 2020), contact tracing is even more effective and convenient with the help of digital instruments.

Indeed, countries with a lower COVID-19 mortality rate seem to have used digital technologies extensively in their pandemic response toolkits (Whitelaw et al., 2020). In South Korea, for instance, PHAs utilized digital technologies to back-track the movements of positive cases in the country by using innovative as well as aggressive methods since the early days of the pandemic: Credit card transactions, mobile location records, and security camera appearances of the patients were inspected, and the extracted data shared with the public in detail in the forms of web-based maps and smartphone applications (Sharon, 2020). Especially on contact tracing, it is argued that conventional practices, which require an *army of detectives* (Sun et al., 2020) to work manually, are time-consuming efforts which are inefficient alone (Almagor & Picascia, 2020; Levy & Stewart, 2020) On the other hand, digital technologies promise to complement the traditional approach by automating this laborious process (Whitelaw et al., 2020; WHO, 2020a). As digital technologies reduce the amount of labor required for manual contact tracing to a great extent, they let the PHAs use human resources more efficiently in their COVID-19 response, which may be seen as an invaluable contribution throughout a pandemic. Hence, global attention has turned to smartphones and mobile applications, a promising duo that may easily trace an individual's contacts (Hsiao et al., 2020; Levy & Stewart, 2020). So, we can say that our study has three main topics to discuss.

1. The Role of Technology in Public Health: Our study explores the ways in which technology can promote public health. This could include a discussion of various apps and other technological tools that have been used to track and contain the spread of diseases like COVID-19. Additionally, our study discusses the potential benefits and drawbacks of relying on technology for public health initiatives.

2. The Ethics and Implications of Using Contact Tracing Apps: This study also explores the ethical

implications of using contact tracing apps like *Hayat Eve Sığar*[1](HES) in Turkey. Additionally, it discusses the potential benefits and drawbacks of using these apps to track and contain the spread of COVID-19. Finally, it suggests ways in which privacy concerns could be addressed while still using these apps.

3. The Impact of Public Perception on the Effectiveness of Contact Tracing Apps: This study explores how public perception of contact tracing apps like HES can influence their effectiveness. Additionally, it discusses the ways in which public health authorities and private organizations can work to improve public trust in these apps. Finally, it suggests ways in which contact tracing apps could be designed to better address public concerns.

LITERATURE REVIEW

In this part, we will first evaluate the technical aspects of different contact tracing mobile applications and then ethical considerations and privacy concerns revolving around these apps. After that, we will give brief information about the HES application and the critics garnered around it.

Contact Tracing Mobile Applications

Contact tracing mobile applications (CTMAs) [Also referred to as, but not limited to, proximity tracing/tracking tools (Abuhammad et al., 2020; WHO, 2020a), participatory disease surveillance systems (Geneviève et al., 2019; Karimuribo et al., 2017), mobile contact tracing applications (Bedogni et al., 2020; Zeinalipour-Yazti & Claramunt, 2020), digital contact tracing (Anglemyer et al., 2020; Ryan, 2020)] are digital instruments developed to probe the proximity of the app users in an automatized way to see if they were exposed to the virus through close-range physical proximity to a COVID-19 positive person.

CTMAs may be developed either by PHAs or private organizations (Levy & Stewart, 2020). In some countries, CTMAs were developed by efforts of national PHAs without using externally available frameworks. Others are the applications developed by adopting the existing frameworks for building contact tracing applications, such as the Exposure Notification application programming interface (API) developed in collaboration by Google and Apple, Decentralized Privacy-Preserving Proximity Tracing (DP-3T) developed collectively by an international consortium of technologists, legal experts, engineers and epidemiologists, and BlueTrace developed by Singapore Government Digital Services.

The Government of Singapore was the first to release a CTMA - as early as March 20, 2020 (Koh, 2020), only nine days after WHO declared COVID-19 as a pandemic (WHO, 2020b) - which is called the TraceTogether app. After that, a frantic flow of mobile applications for contact tracing began. Some examples are the *Aarogya Setu* of India, the *COVIDSafe* app of Australia, the *NHS COVID-19* app of the United Kingdom (UK), the *HaMagen 2.0* of Israel, and the HES app of Turkey.

Operational Differences: Sources of Data

Even though the CTMAs may operate in different ways according to the frameworks they adopt, all of them achieve the objective of tracing the contacts of their users by utilizing one or more of the following assets: Rich sensors and features of smartphones such as Bluetooth technology, a global positioning system (GPS), microphone, and camera (Azad et al., 2020), records of cellular base stations and logs of Wi-Fi signals that a smartphone encountered with (Ahmed et al., 2020). For instance, the NHS COVID-19 app, which has operated through the framework developed by Google/Apple, and the applications TraceTogether & COVIDSafe, which has adopted the BlueTrace framework, had relied on Bluetooth technology (Bay et al., 2020; Google/Apple, 2020a). In both frameworks, smartphones of the app users were constantly transmitting anonymized signals via Bluetooth while collecting the signals transmitted by the users in their vicinity. If, at some point, they get informed - again, anonymously - that the owner of a signal they received was reported positive diagnosis for COVID-19, they could get themselves tested and self-isolated to break the chain of

[1] *Hayat Eve Sığar*, which may be translated as *Life Fits Home*, was also the motto that was frequently used by PHAs in Turkey within the efforts of pandemic management.

transmission.

On the other hand, CTMAs like Aarogya Setu and HaMagen, operating based on the frameworks developed by their national PHAs, utilized Bluetooth technology combined with GPS (MyGov India, 2020; Sokol & Staff, 2020). Using GPS for contact tracing involves the data of the specific location of the app users, whereas solely taking advantage of Bluetooth technology only gives the information on the proximity of the devices. The apps that used Bluetooth-based technology could not collect and process the location data (Google/Apple, 2020b; Sun et al., 2020). Therefore, Bluetooth-based solutions are considered more privacy-preserving (Zhang et al., 2020). In the case of the HES app, which operated through the framework developed by the Ministry of Health of the Turkish Republic, both Bluetooth technology and GPS were known to be used for contact tracing.

Data Storage Approaches

In terms of software architecture, there are two main categories that each CTMA falls under, namely, centralized design and decentralized design (Dar et al., 2020). If a CTMA is centralized by design, that means all the users are connected to a single point of authority with whom they share data regarding their health and location, whereas, in the case of a decentralized design, there is no single authority that can access to all the user data. There were argued to be 120 CTMAs available in 71 countries (Woodhams, 2020). At least 63 CTMAs that were in use in 38 countries adopted the Exposure Notification API (Rahman, 2020), which is a decentralized framework that uses privacy-preserving technologies that operate without collecting the location data of the users (Google/Apple, 2020b). Thus, the CTMAs which adopted it as their core framework are decentralized apps. It is essential to point out that if a user of a decentralized CTMA such as the NHS COVID-19 app tests positive for COVID-19, it is up to them to share this information with their recent contacts that were collected in their device (NHS, n.d.). Moreover, when a user reported that they tested positive, the PHAs were not able to identify the users who had physical contact with the infected user, since the contacts stored in the user's device (Raskar et al., 2020).

The HaMagen app and the CTMAs that adopted the BlueTrace framework, such as TraceTogether and COVIDSafe, also stored the received Bluetooth signals in users' devices. However, they matched the contacts on a centralized server (Levy & Stewart, 2020). Thus, they can be considered partially decentralized. Finally, examples such as Aarogya Setu and the HES app were collecting and processing the data in a centralized manner, which, by far, is the least preferable approach among the options in terms of data security (Ahmed et al., 2020; Cho et al., 2020; Leins et al., 2020; Sun et al., 2020).

As the CTMAs promised significant benefits for public health, they came with the price of risking the personal data of individuals since the collected data had to contain sensitive personal information of the users by its nature. Thus, since the early days of the COVID-19 pandemic, there has been an ongoing debate on CTMAs.

Ethical Considerations & Privacy Concerns Regarding the Contact Tracing Mobile Applications

As Zeinalipour-Yazti and Claramunt put it, the question has been whether the CTMAs should be considered as *a digital vaccine or a privacy demolition* (2020). Naturally, this question has received a sizeable amount of attention from a broad set of critical voices, including influential scholars (e.g., Harari, 2020; Morozov, 2020), journalists (e.g., Ellis-Petersen, 2020; Shevlane et al., 2020; Singer, 2020), international & intergovernmental organizations (e.g., WHO, 2020c), and non-governmental organizations (NGOs) focused on defending human rights (e.g., Future of Privacy Forum, 2020; Human Rights Watch, 2020; Privacy International, 2020). At different levels, all these parties drew attention to - and warned against - the data privacy risks and antidemocratic processes that might arise from the improper use of the CTMAs.

Meanwhile, the *digital vaccine* side of the spectrum mainly consists of government officials worldwide (e.g., AAP, 2020; Busvine et al., 2020a; Koca, 2020). Even though the effectiveness of the CTMAs was backed up with scientific evidence (Ferretti et al., 2020), the above-summarized flow of

information was bearing the risk of shaping public opinion regarding the CTMAs towards a direction in which public health is at stake.

By using an algorithm they developed, a group of researchers from the University of Oxford found that, in the case of the UK, the COVID-19 pandemic could be suppressed technically if 56% of the population - or 80% of the smartphone users - actively used a CTMA (Hinch et al., 2020). The suggested adoption rates should be higher for developing and underdeveloped countries, where internet penetration and smartphone ownership levels are lower than in the UK. One of the fundamental necessities for PHAs to achieve such high adoption rates of CTMAs is establishing public trust regarding the legitimacy and safety of the applications (Ranisch et al., 2020). Thus, for a CTMA to contribute to the fight against a pandemic, the citizens' concerns should be considered by PHAs.

Many attempts have been made within academia to discuss and determine the ethical guidelines to be followed by private organizations and PHAs to develop a rights-based, privacy-preserving, and effective CTMA (e.g., Abuhammad et al., 2020; Gasser et al., 2020; Levy & Stewart, 2020; Lo & Sim, 2020; Morley et al., 2020; Ranisch et al., 2020). These attempts have jointly considered specific technical capabilities and attributes obligatory for an ethically designed CTMA.

One of the first things advocated in the mentioned guidelines is that a CTMA should be open-sourced, i.e., the app's code must be publicly available for inspection for transparency and security reasons. Among the CTMAs and contact tracing framework examples discussed above, all but the HES app was known to be open-sourced.

Another issue commonly pointed out is that the app should anonymize the data collected from users of a CTMA for the sake of personal data privacy. According to the information available on their websites, the NHS COVID-19 app, TraceTogether, and HaMagen 2.0 claimed that they collect and process the personal data of their users with varying degrees of anonymization. However, the concept of anonymity in the digital sphere is known to be a tricky issue (Culnane & Leins, 2020; Sun et al., 2020) since it is proven that the anonymized data can be de-anonymized with the help of specific techniques (Xue et al., 2016; Dar et al., 2020; Leins et al., 2020). Thus, to minimize the privacy risk in a data leak, CTMAs should have collected and processed the minimum possible amount of data, especially if they operate based on a centralized framework (Dumbrava, 2020). On the other hand, as the most data-hungry CTMA among the mentioned examples throughout the research, the HES application did not refer to anonymity in its terms-of-use document[2].

Voluntariness is also a critical point in all the guidelines mentioned above, which defend the necessity of explicit user consent for data collection and processing by a CTMA. European Union Agency For Fundamental Rights (2020) also underlined that downloading and using a CTMA must be the free choice of individuals, thus calling the EU member states to act accordingly. Using the app was voluntary in NHS COVID-19, COVIDSafe, TraceTogether, HaMagen 2.0, and HES applications. Aarogya Setu, on the other hand, was made mandatory with an official guideline on May 1, 2020, by the government of India to the employees of both public and private institutions; later in the same month, the word *mandatory* dropped from the guideline (The Wire, 2020). However, citizens must be informed in advance regarding the app's data policy to decide whether to download the app. A citizen's consent for collecting, for instance, location data cannot be considered valid and voluntary unless the citizen is informed in detail about how their location data will be used. Thus, the HES application was criticized by many, including legal experts, because the privacy policy and the user agreement of the app were not detailed enough (Çayır, 2020a).

Another critical aspect of the concept of voluntariness is the consistency of the conditions that lead to consent that is given. In the case of TraceTogether, even though they assured the citizens earlier that their data would be used only for pandemic management purposes, months after the Government of

[2] Terms-of-use document: https://hayatevesigar.saglik.gov.tr/gizlilik_politikasi_index_V2.html (Accessed on 17 January 2024)

Singapore admitted that the police department might also use the data collected through the CTMA for criminal investigations (Illmer, 2021). Thus, the conditions of the voluntary decision made by more than 70% of the population of Singapore had changed. However, the data collected from the citizens before were still available for the use of the police forces.

The HES Application and the Critical Perspectives

Released on April 17, 2020, the HES application was a CTMA in which the app users - among many side-features (see Çayır, 2020a, p.32-33) - mainly could monitor their status regarding COVID-19, get notified if they were exposed to COVID-19, see the heat maps in which they could see the intensity of the COVID-19 positive cases in a particular area in Turkey. Users could also obtain a HES code through the application, a ten-character combination of random letters and numbers linked to the owner's national identity number. In Turkey, getting a HES code was obligatory during the COVID-19 pandemic for traveling in the country and entering public service buildings, universities, and, occasionally, workplaces. The code could be obtained via the HES application, SMS, or e-Government Gateway.

The features listed above required giving specific permissions to the HES application. For instance, users must have shared their GPS-based location data with the application to see the heat maps. Users must have authorized the application to manage Bluetooth connections to be notified if they had contact with a COVID-19-positive case. Moreover, the app requires the user's national identity number and mobile phone number to start operating. Thus, the application could technically use the cellular base station records for contact tracing. Yet it cannot be known since neither a white paper was available to the public that explains the framework, nor a public announcement was made regarding the issue (Çayır, 2020a). The HES application also required access to the camera, microphone, media gallery, contacts, internal storage, Wi-Fi connections, full network access, and Google service configurations of the device (T.C. Sağlık Bakanlığı, n.d.) to run specific tasks. Thus, it did not comply with the principle of minimum data collection. Also, it was operating through a centralized framework developed by the Ministry of Health of Turkey, which does not anonymize its users (Çayır, 2020a).

In the light of the discussion carried out so far, the CTMAs mentioned previously can be positioned as shown in Figure 1 according to the risks they bear on data privacy. Since it is closed-sourced, centralized, and collecting location data from its users by utilizing GPS, the HES application is positioned in the least privacy-preserving spot.

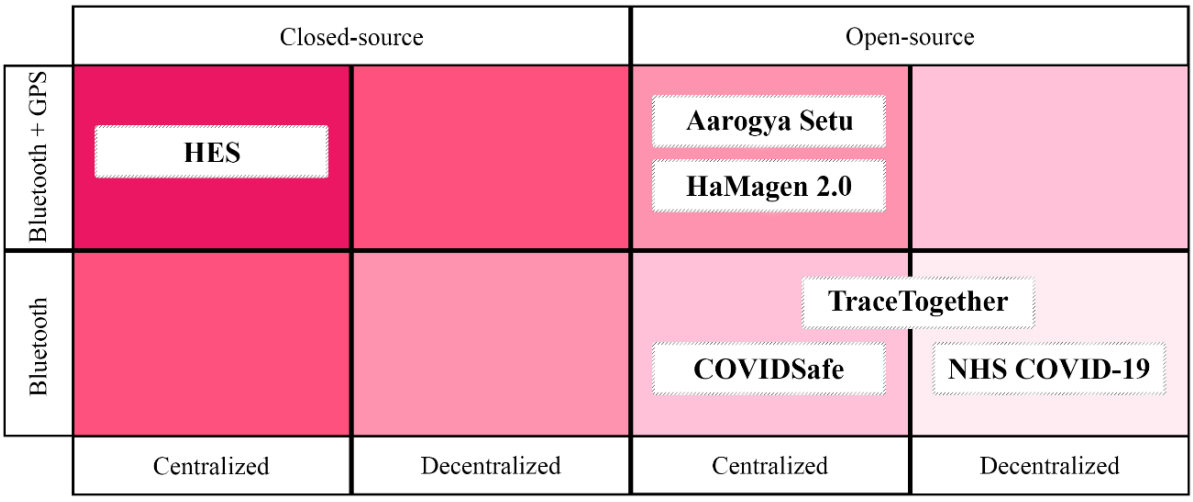


Figure 1. Positioning the contact tracing mobile applications according to their designs
Note. The most privacy-preserving area of the chart is considered to be the lower right corner. Privacy-preservation level decreases as one goes to left and/or up on the chart.

The HES app, downloaded by 40 million citizens as of December 13, 2020 (Hayat Eve Sığar, 2020), has drawn significant criticism since it was published. Several articles, such as those written by Tezcan (2020) and Alan (2020) on digital news outlets like Gazete Duvar, criticized the app. The report from Kasapoğlu (2020) on *BBC News Turkish* criticized how the HES app operated and drew attention to the danger of the normalized invasive digital surveillance practices. Referring to the concept of surveillance for making sense of the COVID-19 crisis was also popular among academics such as Polat (2020), Tokgöz (2020), and Konak & Ertan (2020), who pointed out the risks associated with surveillance technologies that are being used within the COVID-19 response toolkit of the Government of Turkey. Alternative Informatics Association (AIA) - an NGO in Turkey that mainly focuses on subjects such as digital rights, free web, and mass surveillance - published two e-books (see Çayır, 2020a, 2020b) explaining that the HES app was not following a privacy-preserving approach. Therefore, it should be rearranged *in a transparent and auditable manner* (Çayır, 2020a, p.45).

A joint statement, which was signed by more than one hundred organizations around the world, including AIA, was published on April 2, 2020, urging governments to respect human rights while adopting digital technologies to fight the pandemic (Çayır, 2020c; Human Rights Watch, 2020). The declaration defended eight principles that a government or a private organization should meet while developing digital tools to fight the pandemic. According to the report, ethically appropriate pandemic response technologies:

> 1) Are lawful, necessary and proportionate, transparent, and justified by legitimate public health objectives; 2) Are time-bound and only continue for as long as necessary to address the pandemic; 3) Are limited in scope and purpose, used only to respond to the pandemic; 4) Ensure sufficient security of any personal data that is collected; 5) Mitigate any risk of enabling discrimination or other rights abuses against marginalized populations; 6) Are transparent about any data-sharing agreements with other public or private sector entities; 7) Incorporate protections and safeguards against abusive surveillance, and give people access to effective remedies; and 8) Provide for free, active, and meaningful participation of relevant stakeholders in data collection efforts. (Human Rights Watch, 2020)

The principles listed above can be found in the frameworks of most CTMAs. However, in the case of the HES app, since there is neither an open-sourced framework, an illustrative public announcement, nor a detailed privacy policy that explains how the data was collected from the users, it was impossible to assess how ethically appropriate it is.

RESEARCH

We aimed to discover whether the individuals living in Turkey bear the concerns about the concept of contact tracing mobile applications discussed above regarding the HES application released by Turkey's Ministry of Health as a part of their COVID-19 response. While conducting the research, we also tried to understand the relations between the concerns of the individuals associated with the pandemic and their concerns regarding the HES application. Furthermore, we aimed to explore the connections between these concerns and how individuals interacted with the HES application. Thus, we designed an online survey to answer the following research questions:

RQ: Were the users of the HES application having concerns about it?
Sub-RQ1: Were the users of the HES application having concerns about invasive digital surveillance?
Sub-RQ2: Were the users of the HES application having lack of belief in application's legitimacy?

Additionally, we wanted to test the following hypotheses to present a comprehensive understanding of the concerns regarding the HES app and the outcomes of those concerns, which may affect the benefits of the CTMAs on public health:

H1: Individuals' who were more concerned regarding the COVID-19 pandemic were carrying less belief in the legitimacy of HES application.
H2: Individuals' concerns regarding the COVID-19 pandemic were positively correlated with their

concerns about invasive digital surveillance.
H3: Lower levels of belief in the legitimacy of the HES application and the concerns about invasive digital surveillance were positively correlated.
H4: Carrying less belief in the legitimacy of the HES application negatively affected the individuals' decision to download it.
H5: Concerns about invasive digital surveillance negatively affected the individual's decision to download the HES application.
H6: Lower levels of belief in the legitimacy of the HES application caused less frequent use of it.
H7: Concerns about invasive digital surveillance caused less frequent use of the HES application.
H8: Individuals who were more skeptical of the legitimacy of the HES application were more likely to refuse its authorization requests.
H9: Individuals who were more concerned about invasive digital surveillance were more likely to refuse the authorization requests of the HES application.

Sampling

As we previously mentioned, the HES application has downloaded by 40 million citizens as of December 13, 2020 (Hayat Eve Sığar, 2020). Our research focuses on the concerns of individuals living in Turkey about the HES application, which requires a smartphone and a mobile internet access to operate. Hence, the number of mobile internet users in Turkey can also be considered as the population of this research, which was nearly 58 million in 2020 (We Are Social & Hootsuite, 2020, p.25). According to Krejcie and Morgan (1970), to conduct research on a population of this size with a confidence level of 95% and with a margin of error of 5%, the required sample size is at least 384 participants. Initially, 517 individuals participated in our research. We eliminated 60 surveys due to missing data. Thus, our sample consisted of 457 participants. We used simple random sampling method to determine the participants to collect data from. Hence, the research sample may not be as diverse as the user base of HES app, which should be noted as a limitation of our research.

Instrument

We designed an online survey using Google Forms. Using the initial questionnnaire, we conducted a pilot research on thirteen individuals with different demographic characteristics and updated the questions according to the feedback we received. Istanbul Medipol University, Ethical Committee for Scientific Research in Social Sciences granted permission on 22/04/2024 (issue number: 54) to the finalized version of the questionnaire to be used for the purposes of our research. Then, we posted the survey link to various accounts, profiles, groups, and pages on Twitter, Facebook, and LinkedIn. The participants answered the questionnaire between December 13 and December 24, 2020. They were presented with a participation consent page before the questionnaire, which clearly explained that the participation is voluntary, and the data collected through the survey will be used only for research purposes and analyzed anonymously. Thus, we collected the data only from the participants who gave informed consent. The survey consisted of two main sections – The first part included 16 questions on demographics, motivations for downloading and using the HES application, permissions given by the participant to it, and the overall level of concern of the participant regarding the pandemic. The second part consisted of twelve Likert-style questions on a five-point scale to explore the opinions and attitudes of the individuals regarding the HES application.

Research Design

The joint statement mentioned above was our starting point. We prepared survey questions for each of the eight principles in this declaration. While designing this experimental scale, we aimed to explore whether the concerns raised by data privacy experts, law professionals, academics, journalists, NGOs, and international and intergovernmental organizations regarding CTMAs were also perceived by the participants. Hence, our research is a causal, cross-sectional, and quantitative one.

FINDINGS

In this section, we initially introduced the findings of the descriptive analysis of the demographics and the data collected through the survey's Likert-style questions. Then, we presented the findings of the inferential statistic

Most of the sample comprised of female participants (n=279/457). One participant declared their gender as non-binary. Nearly three-quarters of the participants (n=339) were between 21 and 39. 73.1% of the participants were employed or students (n=334). 89.9% of the participants have had a Bachelor's degree or above.

Regarding the financial status, 27.8% of the respondents were earning less than 1501₺ per month, and 58% of the respondents had 2501-11000₺ income per month. As Girgin & Şahin (2020) reported, Turkey's minimum monthly wage in 2020 was 2324₺.

Among the participants, 58.6% (n=268) chose the answer *worried* among the options *not worried*, *worried*, and *too worried* regarding the COVID-19 pandemic. 25.6% of the participants (n=117) chose the answer *too worried*, whereas 15.8% (n=72) chose the answer *not worried*.

The participants were then asked why and when they downloaded the HES application. 11.6% of participants (n=53) declared they had never downloaded it. Answers from the rest of the participants are listed in Table 1.

Table 1. Downloading the HES application: Why & when?

		n	%
I downloaded the HES app…	…to see the intensity of the disease through the heat maps.	222	55
	…out of curiosity.	157	38.9
	…to get an HES code.	131	32.4
	…because it was mandatory for traveling.	115	28.5
	…to get informed if I was potentially exposed to COVID-19.	49	12.1
	… to ease my anxiety regarding the pandemic.	28	6.9
	…upon the recommendations of my family and/or friends.	24	5.9
	…because it is mandatory in my workplace.	16	4
	…after I tested positive for COVID-19.	11	2.7
	…after discovering that I had contact with a positive case.	8	2
	…in April, 2020	75	16.4
	…in May, 2020	122	26.7
	…in June, July, or August, 2020	92	20.1
	…in September or October, 2020	63	13.8
	…in November or December, 2020	31	6.8
	Do not remember	21	4.6

The participants who downloaded the HES application (n=404) were then asked whether they still had it on their devices. 80.4% (n=325) of them responded that they still have it, while 15.1% (n=61) of them answered that they uninstalled it by stating that they did not find it necessary, and 4.5% (n=18) of them said that they uninstalled it because they did not want to continue sharing their data.

Then, they were asked how often they used it. The findings are as follows: 6.8% (n=22) were using it every day, 37.8% (n=123) were using it a couple of times a week, 53.9% (n=175) were using it a couple of times a month, and 1.5% (n=5) were not using it at all.

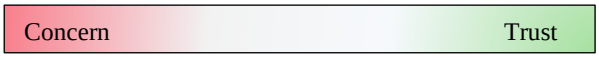
Twelve Likert-style questions that all the participants (n=457) answered are shown in Table 2. All twelve questions' internal consistency (Cronbach's alpha) was 0.914 on our sample, indicating a high level of reliability since it exceeds the recommended minimum of 0.70 (Hair et al., 2014). Moreover,

the Cronbach's Alpha value does not increase with the removal of any items.

In terms of explained variance, our model exhibits considerable explanatory power. Factor 1: *Belief in the Legitimacy of the HES Application* (40%) and Factor 2: *Concerns about invasive digital surveillance* (20.4%) explain more than 60% of the variance in the sample.

Table 2. The items of the Likert-style part of the survey and the factors
Note. (1) strongly agree, (2) agree, (3) not sure, (4) disagree, (5) strongly disagree

Factors	Items	(1) %	(2) %	(3) %	(4) %	(5) %
F1: Belief in the legitimacy of the HES application	V1. I think that disease surveillance activities, such as contact tracking carried out via collecting data from users of the HES app, are legal.	12.7	32.8	35.2	11.6	7.7
	V2. I think that disease surveillance activities such as contact tracking, carried out by collecting data from users of the HES app, aim only to protect and improve public health.	11.2	31.3	31.5	14.4	11.6
	V3. I think the HES app was developed by taking the opinions of representatives from non-governmental organizations, universities, and the private sector.	5	18.6	40.5	21.7	14.2
	V4. I think the purpose of collecting data from users of the HES app and how that data will be used be shared with the citizens clearly.	5	14.7	26.5	28	25.8
	V5. I think the authorities do everything necessary to keep the personal data collected from the users of the HES application safe.	3.5	15.1	33.7	22.8	24.9
	V6. I think the personal data records collected from users of the HES app will be deleted by the authorities when the disease risk ends.	3.5	7	27.8	21.4	40.3
	V7. I think the HES application has significantly contributed to the efforts to combat the pandemic.	12.9	40	28	11.4	7.7
	V8. I like the HES application.	6.3	32.6	35	18.2	7.9
	V9. Poverty-stricken individuals and foreigners living in Turkey also benefit from activities to protect public health through the HES app.	3.1	15.1	30.4	28.4	23
	V10. Considering the HES application, I can say that I would proceed confidently to the new disease surveillance applications to be developed by the authorities for a future pandemic.	6.1	21	44.2	15.1	13.6
F2. Concerns about invasive digital surveillance	V11. I am concerned that the pandemic period will be used as an excuse for indefinite surveillance that governments can implement through surveillance technologies, such as street cameras, smartphone apps, and sensors.	23	32.6	26.7	13.6	4.2
	V12. I think the HES application can access some personal data of its users without their consent.	17.7	32.6	33.9	12.9	2.8



We used colors in Table 2 to better explain the relation of the findings with our research questions: In both *belief in the legitimacy of the HES application* and *concerns about invasive digital surveillance*, the level of concern the research sample exhibited regarding the HES application increases from green (ultimate trust in the HES application) to red (ultimate concern regarding the HES application).

We can say that even though they reported their concerns to some degree for all the items in this part of the survey, participants expressed relatively higher levels of concern for issues mentioned in items V3, V4, V5, V6, V9, V11, and V12.

Table 3. Users' attitudes toward the authorization requests of the HES application
Note. F1: Belief in the legitimacy of the HES app; F2: Concerns about invasive digital surveillance

The authorization requests of the HES application	Yes			Not sure			No, I did not find it necessary			No, I did not want to share my data			P-value	
	%	Mean Rank		%	Mean Rank		%	Mean Rank		%	Mean Rank			
		F1	F2		F1	F2		F1	F2		F1	F2	F1	F2
V1. Location (GPS)	71	152	152	10	170	173	9	160	179	10	241	217	.000	.002
V2. Bluetooth	43	145	151	18	162	170	26	169	152	13	209	212	.001	.001
V3. Camera	15	127	160	28	180	173	37	148	145	20	193	184	.000	.034
V4. Media Gallery	8	108	163	32	179	172	34	145	141	26	183	182	.000	.014
V5. Microphone	7	116	155	34	173	167	34	143	136	25	189	196	.000	.000
V6. Contacts	11	129	160	37	168	158	28	148	143	24	187	194	.005	.004

When the participants who still had the HES application installed on their device (n=325) were asked to provide information regarding the authorization requests of the app that they accepted: Most of the participants expressed that they had been sharing their location data with the HES application (n=233/325). 139 participants stated that they gave authorization to the application for accessing Bluetooth connections of their device.

However, significant opposition to the authorization requests of the application is observed besides GPS and Bluetooth access: More than half of the participants stated that they did not accept the authorization requests of the HES app regarding the last four variables; camera, media gallery, microphone, and contacts (see Table 3).

In addition to expressing their acceptance or refusal of each request, participants were given the opportunity to provide reasons for refusing any of the authorization requests made by the HES application. On average, around one of every ten participants indicated that they did not accept the application's requests to access their GPS and Bluetooth connections for data privacy reasons. When it comes to the authorization requests of the app for accesing the camera, media gallery, microphone, and contacts of the user's device, the refusal rate for privacy reasons climbs to nearly a quarter of the research sample. On the other hand, as presented in the Table 3, the portion of the participants who are *not sure* whether the HES application can access these four functions on their device is considerably higher than the ones who made clear that they *did not want to share their data*.

According to the results of the One-Sample Kolmogorov-Smirnov Test, the distribution of responses given by participants for all items did not conform to a normal distribution (p=0,000). Thus, we made non-parametric Kruskal-Wallis tests to see whether there is a significant difference among groups of respondents based on their chosen options for each authorization request of the HES application. Specifically, we investigated whether this difference correlates with the level of concern they exhibit in terms of both F1 (*belief in the legitimacy of the HES application*) and F2 (*concerns about invasive digital surveillance*).

According to the test results, there is a significant difference between users' attitudes towards the authorization requests of the HES application in relation to the level of concern they have for both

factors. Respondents who said, *No, I did not want to share my data*, had significantly the highest degree of disagreement regarding *belief in the legitimacy of the HES application*, as well as the highest degree of having *concerns about invasive digital surveillance* among all ($p<0.05$). In conclusion, the results indicate that the participants who were concerned more about the HES application were less willing to accept its authorization requests, prioritizing the protection of their data privacy.

Analyses of the Hypotheses of the Research

The relations between the variables are illustrated in Figure 2, which indicates different levels of significant correlations.

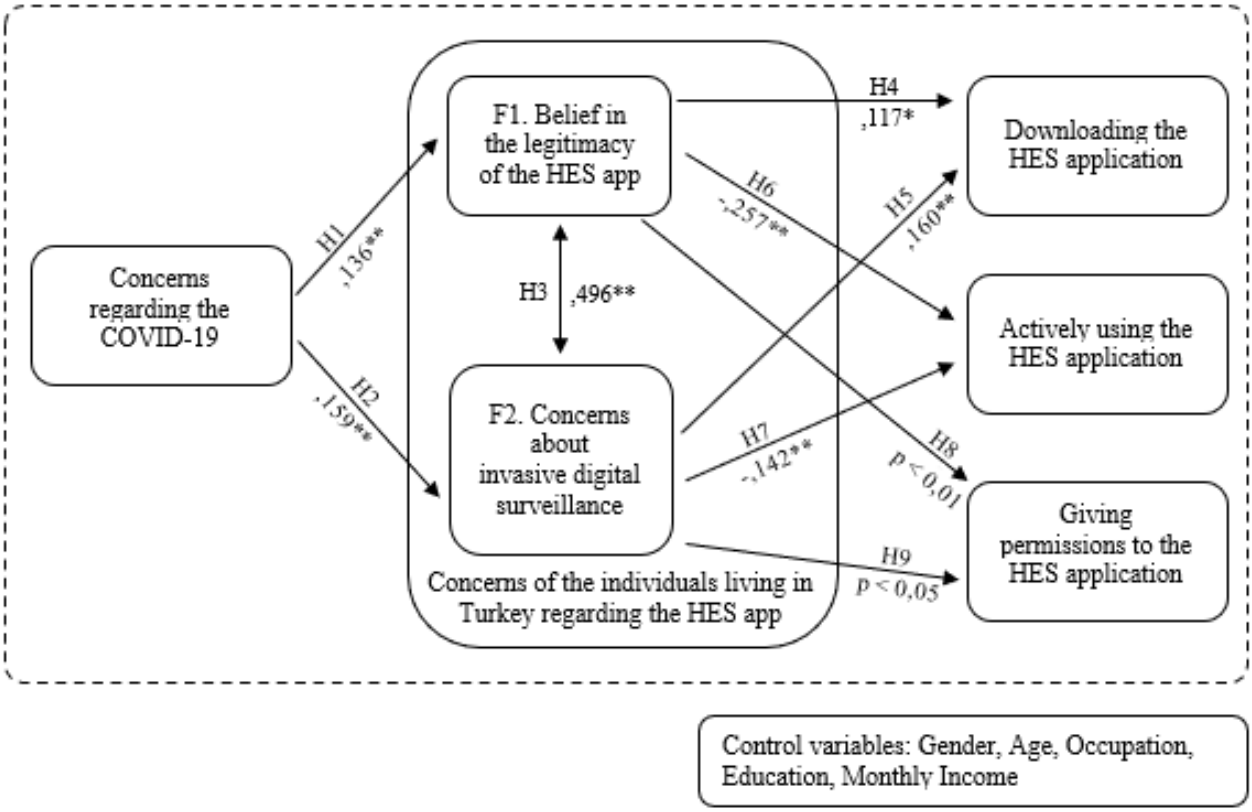


Figure 2. Analysis results of the research model
Note. *: $p<0.05$, **: $p<0.01$

Correlations observed in H4 (rho=,117; $p<0,05$) and H5 (rho=,160; $p<0,01$) explain the relationship between the level of concern of the individuals and the month they downloaded the HES app; the individuals who were more concerned regarding the app tended to download it in a later month.

Regarding H6 (rho=-,257; $p<0,01$) and H7 (rho=-,142; $p<0,01$), the correlations shown in Figure 2 indicate that a higher level of concern resulted in less frequent use of HES application. Additionally, we found a very significant difference between the individuals who uninstalled the application, i.e., not using it anymore (Mean Rank=233,16) and those who did not (Mean Rank=195,05) in terms of the belief in the legitimacy of the HES application (Mann-Whitney U=10415,5; $p<0.01$), which further supports hypothesis 6 by pointing out that individuals who had lower levels of belief in the legitimacy of the HES application tend to uninstall it.

Regarding H8 and H9, we observed statistically significant difference between the users who approved the authorizations requested by the HES application and those who did not because of privacy reasons in terms of both factors; belief in the legitimacy of the HES apllication, and concerns about invasive digital surveillance (see Table 3).

We tested five control variables, namely, gender, age, occupation, education, and monthly income. According to our findings, gender, monthly income, and education had no significant relationships with any of the factors. Age, however, had a very significant positive correlation with the lower of belief in the legitimacy of the HES application (rho=,136; $p<0.01$), meaning that older people were more skeptical regarding the app. Age had no significant relationship with having concerns about digital invasive surveillance. On the other hand, participants showed statistically significant differences in their belief in the legitimacy of the HES application according to their occupations. Both retired people and unemployed individuals were more concerned about the HES application (Factor 1 $H=15927$, $p<0.01$, Factor 2 $H=12067$, $p<0.05$) compared to the other three occupation groups. In other words, retired people and unemployed individuals had less belief in the legitimacy of the HES application. They also had more concern about invasive digital surveillance. In light of the analyses we carried out, it can be stated that all 9 of our hypotheses were accepted with evidence.

Discussion

Our research findings indicate that individuals living in Turkey had concerns regarding the HES application. The concerns about invasive digital surveillance practices that the state authorities can enforce through HES or HES-like applications was much more prevalent than the disbelief in the legitimacy of the HES application. Thus, both our research question (*were the users of the HES application having concerns about it?*), and sub-questions (*were the users of the HES application having concerns about invasive digital surveillance? & having lack of belief in application's legitimacy?*) were answered positively.

Furthermore, our findings suggest that the concerned individuals were not simply members of a particular social stratum, meaning that the concerns regarding the HES application were prevalent throughout society. On average, only three out of 10 participants (see the green and bright green columns in Table 2) expressed that they are somewhat comfortable with the HES application.

The findings also exhibit the most important reasons underlying the concerns of individuals regarding the HES application as lack of transparency (V3, V4), risks regarding the security of personal data (V5), mistrust for the time limit of the collected personal data (V6), discrimination against people living in poverty and the foreigners (V9), increased surveillance powers of the state (V11), and suspicion that the application has unauthorized access to devices (V12). These concerns directly related with the principles listed in the joint statement declared by NGOs worldwide, demanding governments to act ethically when responding to the COVID-19 pandemic with digital technologies. Hence, most participants did not seem to think the HES application was ethically designed or respects human rights.

The concerns regarding the HES application posed many negative consequences for its adoption. According to our findings, individuals who were more concerned tend to either not download the application or postpone downloading it for a long time. Upon downloading, concerned individuals have avoided approving the authorization demands of the application (see Table 3), preventing the HES application from properly functioning to trace contacts. Also, concerned individuals used the application considerably less often or even deleted it altogether. Thus, by arousing concerns in the individuals, the HES application made it difficult for PHAs to achieve their objectives of contributing to public health by using a CTMA.

Even though individuals had concerns with the HES application, around 70% of the mobile internet users living in Turkey downloaded it, according to the official numbers declared by Turkey's PHAs. Our findings indicate that the two most prevalent reasons (see Table 1) behind this massive adoption rate were mainly related to seeing heat maps (55%) or out of curiosity (38.9%) rather than personal health benefits, public health benefits, or compulsory circumstances. The third most prevalent reason is getting an HES code (32%), was particularly interesting because using the HES application was not the only way to obtain an HES code. This finding may be pointing out to the insufficient awareness of the participants on data privacy.

CONCLUSION

In this study, we wanted to explore the concerns of people in Turkey regarding the HES appl through a critical as well as utilitarian perspective. The results of our research indicate that despite its high adoption rate, the HES application is far from being a service that the public trusts without question. The majority of the citizens who were using the application throughout the COVID-19 pandemic were using it with various degrees of concern. Therefore, we suggest that health crises should not be used as excuses for the increased implementation of digital surveillance technologies on citizens without consensus being reached through civic engagement. Health crises should not be used as a legitimizing tool for restricting individual rights and breaching data privacy.

According to our results, a large percentage of the individuals expressed that they were in a state of indecision concerning the legitimacy of the HES application, meaning that they neither agreed nor disagreed that the HES application was legitimate. We evaluate and interpret this result in connection with the occurrence of a pandemic and the concerns it aroused among individuals. When a highly contagious, deadly virus hit the world, it got more complicated for the citizens to decide which intervention was legitimate and which was not. Thus, digital technologies for a pandemic response should not force individuals to choose between two fundamental human rights: Their right to live a healthy life and their right to privacy.

We argue that the use of technology in the form of CTMAs might promote public health. This could include various apps and other technological tools that have been used to track and contain the spread of diseases like COVID-19. Besides its certain benefits, there are obvious drawbacks of relying on technology for public health initiatives. Our study revealed with evidence that people in Turkey had concerns about the ethical implications of using contact tracing apps, such as the HES application. Similar studies conducted in the United Kingdom, Germany, Italy (Altmann et al., 2021), the United States, France, and Australia (Chan & Saqib, 2021), also presented similar findings and identified concerns regarding cyber security & data privacy, and lack of belief in the authorities, as among the most important barriers that may hinder the adoption of such applications by citizens. These concerns seem to have negatively impacted citizen's trust in the CTMAs worldwide, and consequently limited its potential benefits. To eliminate the portrayed negative public perception, public health authorities and private organizations must work to improve public trust in these applications. In line with the literature, we also argue that the PHAs in Turkey should revise the application's architecture and reorganize it in a decentralized, transparent, auditable, privacy-preserving manner for possible future health crises to serve the public health better.

While our study presents valuable insights regarding the perspectives of the citizens of Turkey about digital surveillance technologies through the lens of HES application, it has limitations. The diversity of the research sample was not as desired, since the data of our research was collected with online tools due to lockdown measures that were effective back in the time of data collection. Hence, it may limit the generalizability of our findings. For future research, we suggest having a more diverse sample to enhance the representative capacity of the results.

Finally, personal data privacy in the digital sphere is not just a problem specific to times of the COVID-19 pandemic but also concerns the future. It is crucial to provide individuals with the necessary information, education, and tools that would help them maintain their data privacy.

REFERENCES

AAP. (2020, April 27). 2 million download virus apps. PerthNow. https://www.perthnow.com.au/news/coronavirus/aussies-praised-as-more-than-two-million-download-covidsafe-contact-tracing-app-ng-b881531548z

Abuhammad, S., Khabour, O. F., & Alzoubi, K. H. (2020). COVID-19 Contact-Tracing Technology: Acceptability and Ethical Issues of Use. Patient Preference and Adherence, 14, 1639–1647. 10.2147/PPA.S276183

Ahmed, N., Michelin, R. A., Xue, W., Ruj, S., Malaney, R., Kanhere, S. S., Seneviratne, A., Hu, W.,

Janicke, H., & Jha, S. (2020). A Survey of COVID-19 Contact Tracing Apps. IEEE Access, 8, 134577–134601. 10.1109/ACCESS.2020.3010226

Alan, S. (2020, May 25). HES uyarısı: Kişisel verilerin gizliliği ihlal edilebilir. Gazete Duvar. https://www.gazeteduvar.com.tr/gundem/2020/05/25/hes-uyarisi-kisisel-verilerin-gizliligi-ihlal-edilebilir

Almagor, J., & Picascia, S. (2020). Exploring the effectiveness of a COVID-19 contact tracing app using an agent-based model. Scientific Reports, 10(1), 22235. 10.1038/s41598-020-79000-y

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

Anglemyer, A., Moore, T. H., Parker, L., Chambers, T., Grady, A., Chiu, K., Parry, M., Wilczynska, M., Flemyng, E., & Bero, L. (2020). Digital contact tracing technologies in epidemics: A rapid review. Cochrane Database of Systematic Reviews, 8. 10.1002/14651858.CD013699

Azad, M. A., Arshad, J., Akmal, S. M. A., Riaz, F., Abdullah, S., Imran, M., & Ahmad, F. (2020). A First Look at Privacy Analysis of COVID-19 Contact Tracing Mobile Applications. IEEE Internet of Things Journal, 1–1. 10.1109/JIOT.2020.3024180

Bay, J., Kek, J., Tan, A., Hau, C. S., Yongquan, L., Tan, J., & Quy, T. A. (2020). BlueTrace: A privacy-preserving protocol for community-driven contact tracing across borders. https://bluetrace.io/static/bluetrace_whitepaper-938063656596c104632def383eb33b3c.pdf

Bedogni, L., Rumi, S. K., & Salim, F. (2020). Modeling Memory for Individual Re-identification in Decentralised Mobile Contact Tracing Applications. http://arxiv.org/abs/2010.05514

Busvine, D., Alkousaa, R., & Harvey, J. (2020a, June 17). The German coronavirus tracing app downloaded 6.5 million times. Reuters. https://www.reuters.com/article/us-health-coronavirus-germany-app-idUSKBN23O13G

Busvine, D. (2020b, April 22). Switzerland, Austria align with 'Gapple' on corona contact tracing. Reuters. https://www.reuters.com/article/health-coronavirus-europe-tech-idUSL3N2CA36L

Çayır, F. (2020a). Pandemic Tracking Apps and Monitoring of Personal Data Report. Alternatif Bilişim Derneği. https://ekitap.alternatifbilisim.org/covid19-pandemic-tracking-apps-report

Çayır, F. (2020b). COVID-19 Sürecinde Temas Takip Uygulamaları ve Kişisel Verilerin Korunması. Alternatif Bilişim Derneği. https://ekitap.alternatifbilisim.org/covid-19-temas-takip-uygulamalari

Çayır, F. (2020c, October 12). COVID-19 ile mücadelede dijital hak ve özgürlüklere saygı. Alternatif Bilişim Derneği. https://alternatifbilisim.org/covid-19-ile-mucadele-dijital-hak-ve-ozgurluklere-saygi

Chan, E. Y., & Saqib, N. U. (2021). Privacy concerns can explain unwillingness to download and use contact tracing apps when COVID-19 concerns are high. Computers in Human Behavior, 119, 106718. 10.1016/j.chb.2021.106718

Cho, H., Ippolito, D., & Yu, Y. W. (2020). Contact Tracing Mobile Apps for COVID-19: Privacy Considerations and Related Trade-offs. http://arxiv.org/abs/2003.11511

Clarke, J. (1998). Contact tracing for chlamydia: Data on effectiveness. International Journal of STD & AIDS, 9(4), 187–191. 10.1258/0956462981921945

Culnane, C., & Leins, K. (2020). Misconceptions in Privacy Protection and Regulation. Law in Context, 36(2), 49–60. 10.26826/law-in-context.v36i2.110

Dar, A. B., Lone, A. H., Zahoor, S., Khan, A. A., & Naaz, R. (2020). Applicability of mobile contact tracing in fighting pandemic (COVID-19): Issues, challenges and solutions. Computer Science Review, 38, 100307. https://doi.org/10.1016/j.cosrev.2020.100307

Dijk, J. Van. (2020). The Network Society. SAGE.

Donnelly, C. A., Ghani, A. C., Leung, G. M., Hedley, A. J., Fraser, C., Riley, S., Abu-Raddad, L. J., Ho, L.-M., Thach, T.-Q., Chau, P., Chan, K.-P., Lam, T.-H., Tse, L.-Y., Tsang, T., Liu, S.-H., Kong, J. H., Lau, E. M., Ferguson, N. M., & Anderson, R. M. (2003). Epidemiological determinants of spread of causal agent of severe acute respiratory syndrome in Hong Kong. The Lancet, 361(9371), 1761–1766. 10.1016/S0140-6736(03)13410-1

Dumbrava, C. (2020). Lifting coronavirus restrictions: The role of therapeutics, testing, and contact tracing apps: in-depth analysis. https://data.europa.eu/doi/10.2861/7568

Eames, K. T. D., & Keeling, M. J. (2003). Contact tracing and disease control. Proceedings of the

Royal Society of London. Series B: Biological Sciences, 270(1533), 2565–2571. 10.1098/rspb.2003.2554

Ekong, I., Chukwu, E., & Chukwu, M. (2020). COVID-19 Mobile Positioning Data Contact Tracing and Patient Privacy Regulations: Exploratory Search of Global Response Strategies and the Use of Digital Tools in Nigeria. JMIR MHealth and UHealth, 8(4), e19139. 10.2196/19139

Ellis-Petersen, H. (2020, May 4). India's COVID-19 app fuels worries over authoritarianism and surveillance. The Guardian. https://www.theguardian.com/world/2020/may/04/how-safe-is-it-really-privacy-fears-over-india-coronavirus-app

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

Future of Privacy Forum. (2020, March 25). A Closer Look at Location Data: Privacy and Pandemics. Future of Privacy Forum. https://fpf.org/blog/a-closer-look-at-location-data-privacy-and-pandemics

Gandhi, M., Yokoe, D. S., & Havlir, D. V. (2020). Asymptomatic Transmission, the Achilles' Heel of Current Strategies to Control Covid-19. New England Journal of Medicine. 10.1056/NEJMe2009758

Gasser, U., Ienca, M., Scheibner, J., Sleigh, J., & Vayena, E. (2020). Digital tools against COVID-19: Framing the ethical challenges and how to address them. http://arxiv.org/abs/2004.10236

Geneviève, L. D., Martani, A., Wangmo, T., Paolotti, D., Koppeschaar, C., Kjelsø, C., Guerrisi, C., Hirsch, M., Woolley-Meza, O., Lukowicz, P., Flahault, A., & Elger, B. S. (2019). Participatory Disease Surveillance Systems: Ethical Framework. Journal of Medical Internet Research, 21(5), e12273. 10.2196/12273

Girgin, Y., & Sahin, T. (2020, December 28). Turkey to raise minimum wage by 21.56% in 2021. Anadolu Agency. https://www.aa.com.tr/en/economy/turkey-to-raise-minimum-wage-by-2156-in-2021/2090819

Google/Apple. (2020a). Contact Tracing—Bluetooth Specification v1.1. https://blog.google/documents/58/Contact_Tracing_-_Bluetooth_Specification_v1.1_RYGZbKW.pdf

Google/Apple. (2020b, May 20). Exposure Notification API launches to support public health agencies. https://blog.google/inside-google/company-announcements/apple-google-exposure-notification-api-launches

Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2014). Multivariate Data Analysis: Pearson New International Edition (7th Edition). Pearson Education Limited.

Harari, Y. N. (2020, March 20). Yuval Noah Harari: The world after coronavirus. Financial Times. https://www.ft.com/content/19d90308-6858-11ea-a3c9-1fe6fedcca75

Hayat Eve Sığar. [_hayatevesigar]. (2020, December 14). Pandemiyle mücadelemiz sürüyor. Oluşturulan 92 milyon HES Kodu, 1.3 milyar kez sorgulandı. #HESKodu #hayatevesığar [Tweet]. https://twitter.com/_hayatevesigar/status/1338044578226724864

Hinch, R., Probert, W., Nurtay, A., Kendall, M., Wymant, C., Hall, M., Lythgoe, K., Cruz, A. B., Zhao, L., Stewart, A., Ferretti, L., Parker, M., Meroueh, A., Mathias, B., Stevenson, S., Montero, D., Warren, J., Mather, N. K., Finkelstein, A., … Fraser, C. (2020). Effective Configurations of a Digital Contact Tracing App: A report to NHSX. https://cdn.theconversation.com/static_files/files/1009/Report_-_Effective_App_Configurations.pdf

Hsiao, H.-C., Huang, C.-Y., Hong, B.-K., Cheng, S.-M., Hu, H.-Y., Wu, C.-C., Lee, J.-S., Wang, S.-H., & Jeng, W. (2020). An Empirical Evaluation of Bluetooth-based Decentralized Contact Tracing in Crowds. http://arxiv.org/abs/2011.04322

Human Rights Watch. (2020, April 2). Governments Should Respect Rights in COVID-19 Surveillance. https://www.hrw.org/news/2020/04/02/governments-should-respect-rights-covid-19-surveillance

Illmer, A. (2021, January 5). Singapore reveals COVID privacy data available to police. BBC News. https://www.bbc.com/news/world-asia-55541001

Karimuribo, E. D., Mutagahywa, E., Sindato, C., Mboera, L., Mwabukusi, M., Kariuki Njenga, M., Teesdale, S., Olsen, J., & Rweyemamu, M. (2017). A Smartphone App (AfyaData) for

Innovative One Health Disease Surveillance from Community to National Levels in Africa: Intervention in Disease Surveillance. JMIR Public Health and Surveillance, 3(4), e94. 10.2196/publichealth.7373

Kasapoğlu, Ç. (2020, May 13). Türkiye ve dünyadaki temas takip uygulamaları güvenli mi, hak ve mahremiyet ihlallerine yol açar mı? BBC News Türkçe. https://www.bbc.com/turkce/haberler-dunya-52638919

Koca, F. (2020). Turkey's Management of Covid-19: Measures and Strategies of Health Policies. Insight Turkey, 22(Summer 2020), 55–65. 10.25253/99.2020223.04

Koh, D. (2020, March 20). Singapore government launches new app for contact tracing to combat spread of COVID-19. MobiHealthNews. https://www.mobihealthnews.com/news/asia-pacific/singapore-government-launches-new-app-contact-tracing-combat-spread-covid-19

Konak, N., & Ertan, C. (2020). COVID-19 Pandemisi ve Beden-İktidar İlişkisi: Foucaultcu Bir Analiz. Kuram ve Uygulamada Sosyal Bilimler Dergisi. 4(2), 26-40. 10.48066/kusob.827565

Krejcie, R. V., & Morgan, D. W. (1970). Determining Sample Size for Research Activities. Educational and Psychological Measurement, 30(3), 607–610. 10.1177/001316447003000308

Leins, K., Culnane, C., & Rubinstein, B. I. (2020). Tracking, tracing, trust: Contemplating mitigating the impact of COVID-19 with technological interventions. Medical Journal of Australia, 213(1), 6-8.e1. 10.5694/mja2.50669

Levy, B., & Stewart, M. (2020). A Systematic Review of the Ethics and Efficacy of Digital Contact Tracing Applications. Harvard Data Science Review. 10.13140/RG.2.2.23432.85766

Lo, B., & Sim, I. (2020). Ethical Framework for Assessing Manual and Digital Contact Tracing for COVID-19. Annals of Internal Medicine. 10.7326/M20-5834

Loayza, N. V. (2020). Costs and Trade-Offs in the Fight against the COVID-19 Pandemic: A Developing Country Perspective. https://openknowledge.worldbank.org/handle/10986/33764

Morley, J., Cowls, J., Taddeo, M., & Floridi, L. (2020). Ethical guidelines for COVID-19 tracing apps. Nature, 582(7810), 29–31. 10.1038/d41586-020-01578-0

Morozov, E. [evgenymorozov]. (2020, April 10). The nine most terrifying words in the English language are… [Tweet]. https://twitter.com/evgenymorozov/status/1248659080442494976 Accessed on 17 January 2024.

MyGov India. (2020, April 24). Aarogya Setu App | English Version [Video]. YouTube. https://www.youtube.com/watch?v=phc1UAQQ81s&feature=emb_title Accessed on 17 January 2024.

NHS. (n.d.). If I test positive for coronavirus (COVID-19), how does the NHS COVID-19 app alert people who I've been in close contact with?. COVID-19 app support. https://faq.covid19.nhs.uk/article/KA-01356/en-us?parentid=CAT-01033&rootid=. Accessed on 17 January 2024.

Oran, D. P., & Topol, E. J. (2020). Prevalence of Asymptomatic SARS-CoV-2 Infection: A Narrative Review. Annals of Internal Medicine, 173(5), 362–367. 10.7326/M20-3012

Polat, N. (2020). Dijital pandemi gözetimi, beden politikaları ve eşitsizlikler. Kültür ve Siyasette Feminist Yaklaşımlar, 41, 94–107.

Privacy International. (2020, April 2). Civil Society Sound Alarm Over Unprecedented Global Wave of Surveillance in Fight Against COVID-19. Privacy International. http://privacyinternational.org/press-release/3581/civil-society-sound-alarm-over-unprecedented-global-wave-surveillance-fight

Rahman, M. (2020, December 28). List of countries using Google and Apple's COVID-19 Contact Tracing API. https://www.xda-developers.com/google-apple-covid-19-contact-tracing-exposure-notifications-api-app-list-countries

Ranisch, R., Nijsingh, N., Ballantyne, A., van Bergen, A., Buyx, A., Friedrich, O., Hendl, T., Marckmann, G., Munthe, C., & Wild, V. (2020). Digital contact tracing and exposure notification: Ethical guidance for trustworthy pandemic management. Ethics and Information Technology. 10.1007/s10676-020-09566-8

Raskar, R., Schunemann, I., Barbar, R., Vilcans, K., Gray, J., Vepakomma, P., Kapa, S., Nuzzo, AGupta, R., Berke, A., Greenwood, D., Keegan, C., Kanaparti, S., Beaudry, R., Stansbury, D., Arcila, B. B., Kanaparti, R., Pamplona, V., Benedetti, F. M., … Werner, J. (2020). Apps Gone Rogue: Maintaining Personal Privacy in an Epidemic. http://arxiv.org/abs/2003.08567

Sharon, A. (2020, March 14). South Korea looks to tech to combat Covid-19. OpenGov Asia. https://opengovasia.com/south-korea-looks-to-tech-to-combat-covid-19

Shevlane, T., Garfinkel, B., & Dafoe, A. (2020, April 28). Contact tracing apps can help stop coronavirus. But they can hurt privacy. Washington Post. https://www.washingtonpost.com/politics/2020/04/28/contact-tracing-apps-can-help-stop-coronavirus-they-can-hurt-privacy

Singer, N. (2020, July 8). Virus-Tracing Apps Are Rife With Problems. Governments Are Rushing to Fix Them. The New York Times. https://www.nytimes.com/2020/07/08/technology/virus-tracing-apps-privacy.html

Sokol, S., & Staff, T. (2020, July 27). Health Ministry launches revamped COVID-19 tracking app. https://www.timesofisrael.com/health-ministry-launches-revamped-covid-19-tracking-app

Sun, R., Wang, W., Xue, M., Tyson, G., Camtepe, S., & Ranasinghe, D. C. (2020). An Empirical Assessment of Global COVID-19 Contact Tracing Applications. http://arxiv.org/abs/2006.10933

T.C. Sağlık Bakanlığı. (n.d.). Hayat Eve Sığar. Google Play Store. https://play.google.com/store/apps/details?id=tr.gov.saglik.hayatevesigar&hl=tr&gl=TR

Tezcan, M. (2020, April 30). Korona günlerinde takip edeni takip edelim. Gazete Duvar. https://www.gazeteduvar.com.tr/teknoloji/2020/04/30/korona-gunlerinde-takip-edeni-takip-edelim

The Wire. (2020, May 17). New Guidelines See Home Ministry Ease Up on Compulsory Use of Aarogya Setu in Offices. The Wire. https://thewire.in/government/in-new-guidelines-home-ministry-eases-up-on-compulsory-use-of-aarogya-setu-in-offices

Tokgöz, C. (2020). COVID-19 İle Mücadelede Konumsal Gözetimin Kurumsallaşması. Kültür ve İletişim. 10.18691/kulturveiletisim.739277

We Are Social & Hootsuite. (2020). Digital in 2020: Turkey. https://datareportal.com/reports/digital-2020-turkey

Whitelaw, S., Mamas, M. A., Topol, E., & Van Spall, H. G. C. (2020). Applications of digital technology in COVID-19 pandemic planning and response. The Lancet Digital Health, 2(8), e435–e440. 10.1016/S2589-7500(20)30142-4

WHO. (2020a). Digital tools for COVID-19 contact tracing: Contact tracing in the context of COVID-19. https://www.who.int/publications/i/item/WHO-2019-nCoV-Contact_Tracing-Tools_Annex-2020.1

WHO. (2020b, March 11). WHO Director-General's opening remarks at the media briefing on COVID-19. https://www.who.int/director-general/speeches/detail/who-director-general-s-opening-remarks-at-the-media-briefing-on-covid-19---11-march-2020

WHO. (2020c, November 19). Joint Statement on Data Protection and Privacy in the COVID-19 Response. https://www.who.int/news/item/19-11-2020-joint-statement-on-data-protection-and-privacy-in-the-covid-19-response

Woodhams, S. (2020, October 13). COVID-19 Digital Rights Tracker. https://www.top10vpn.com/research/investigations/covid-19-digital-rights-tracker

Xue, M., Ballard, C., Liu, K., Nemelka, C., Wu, Y., Ross, K., & Qian, H. (2016). You Can Yak but You Can't Hide: Localizing Anonymous Social Network Users. Proceedings of the 2016 Internet Measurement Conference, 25–31. 10.1145/2987443.2987449

Zeinalipour-Yazti, D., & Claramunt, C. (2020). COVID-19 Mobile Contact Tracing Apps (MCTA): A Digital Vaccine or a Privacy Demolition? 21st IEEE International Conference on Mobile Data Management (MDM), 1–4. 10.1109/MDM48529.2020.00020

Zhang, B., Kreps, S., McMurry, N., & McCain, R. M. (2020). Americans' perceptions of privacy and surveillance in the COVID-19 pandemic. PLOS ONE, 15(12), e0242652. 10.1371/journal.pone.0242652