STUDIA I ANALIZY NAUK O POLITYCE
1 (2023)

https://doi.org/10.31743/sanp.16189

Digital Literacy and Awareness of User Location Privacy: What People in Turkey Know About Google COVID-19 Community Mobility Reports?

Umiejętności cyfrowe i świadomość prywatności lokalizacji użytkownika: Co ludzie w Turcji wiedzą o raportach mobilności społeczności Google COVID-19?

İlknur Nina Paslanmaz Uluğ
Informatics PhD. Candidate, Marmara University, Social Sciences Institute
e-mail: ilknur.ninaa@gmail.com
https://orcid.org/0000-0001-8847-5534

Cem Sefa Sütcü
Prof. Dr., Marmara University, Faculty of Communications, Informatics Department
e-mail: csutcu@marmara.edu.tr
https ://orcid.org/ 0000-0002-9389-6832

Abstract: At the outbreak of the COVID-19, governments, health organizations and large technology companies were not prepared for the measures to be taken against the disease. Contact tracking was widely carried out using location data to prevent the spread of COVID-19 with the use of technological tools, especially smartphones. In this epidemic, economic difficulties also emerged due to the lockdown imposed by the governments. For this reason, social distancing and contact tracing applications have become widespread in order to prevent the disease as soon as possible. Such strategies negatively affected individuals' perceptions of privacy, because authorities gave priority to collecting data from individuals in order to prevent the epidemic. On the other hand, non-governmental organizations suggested that "privacy-first" and "decentralized" approaches should be preferred instead of "data-first" and "centralized" approaches. In this direction, Google and Apple companies have developed a decentralized common API to help fight the virus, which also complies with the European Union's General Data Protection Regulation. And in particular, Google has regularly shared Google Community Mobility Reports (GCMR) publicly by anonymizing the data it collects from Google Maps. Using these reports people and authorities can get movement data about different categories of places such as retail and recreation, supermarkets and pharmacies, parks, public transport, workplaces and residential.

Our aim is to find out whether individuals in Turkey are aware that their location and movement data are being tracked by Google Maps and contact tracing apps for preventing the spread of COVID-19. We also examined their motivations for downloading location

tracing apps and whether they have been taking necessary steps to protect their privacy. We investigated whether they had concerns about the possible future use of contact tracing data collected by the health authorities in Turkey and other institutions like Google.

The scope of the study covers smartphone users. We collected data through an online survey using Google Forms. Our survey consists mostly of narrative questions, where we asked respondents to imagine various scenarios where app manufacturers, mobile phone operators/manufacturers, or the government were using some of their data to study or mitigate the spread of COVID-19. Then, between December 15, 2020, and January 2, 2021 we distributed the survey link to the participants through various social media networks. We reported the results of the data of 444 people collected anonymously by quantitative analysis methods.

As a result of the study, it was determined that the digital literacy levels of the individuals are high due to their high education level. Despite this, it has been revealed that the participants do not read the terms and conditions offered in apps. Individuals who care about privacy expressed their willingness to share their data for the sake of public health. As an answer to the main question of our study, it was concluded that the participants' knowledge of GCMR was insufficient. As a matter of fact, it was understood that individuals were indecisive and worried about the use of their data by the authorities in the future due to the uncertainty experienced during the pandemic period.

Keywords: COVID-19, Google Community Mobility Reports, Digital Literacy, Digital Privacy, Location Data Privacy, Technological Change

Streszczenie: W momencie wybuchu pandemii COVID-19 ani władze państwowe, ani zakłady opieki zdrowotnej, ani duże firmy technologiczne nie były przygotowane na podjęcie walki z tą chorobą. Aby zapobiec rozprzestrzenianiu się COVID-19, na szeroką skalę prowadzono kontrolę kontaktów międzyludzkich za pomocą danych o lokalizacji, głównie narzędzi technologicznych, zwłaszcza smartfonów. Podczas pandemii z powodu blokady narzuconej przez rządy pojawiły się m.in. trudności gospodarcze. Z tej przyczyny aplikacje dystansowania społecznego i śledzenia kontaktów stały się powszechne, aby jak najszybciej zapobiec chorobie. Takie strategie negatywnie wpłynęły na postrzeganie prywatności przez jednostki, ponieważ władze nadały priorytet zbieraniu danych od osób fizycznych w celu zapobiegania pandemii. Z drugiej strony organizacje pozarządowe zasugerowały, że preferowane powinno być podejście „przede wszystkim prywatność" i „zdecentralizowanie" zamiast „przede wszystkim dane" i „scentralizowanie". Aby pomóc w walce z wirusem, firmy Google i Apple opracowały zdecentralizowany wspólny interfejs API, zgodny także z ogólnym rozporządzeniem Unii Europejskiej o ochronie danych. W szczególności Google regularnie udostępniało publicznie raporty mobilności społeczności Google (ang. Google Community Mobility Reports – GCMR), anonimizując dane gromadzone z Map Google. Korzystając z tych raportów, użytkownicy uzyskiwali dane dotyczące ruchu w takich kategoriach miejsc, jak: handel detaliczny i rekreacja, supermarkety i apteki, parki i transport publiczny, miejsca pracy i zamieszkania.

Problem badawczy artykułu stanowi następujące pytanie: Czy osoby mieszkające w Turcji były świadome, że ich dane o lokalizacji i ruchu są śledzone przez Mapy Google i aplikacje do śledzenia kontaktów w celu zapobiegania rozprzestrzenianiu się COVID-19? Autorzy artykułu zbadali również motywacje Turków do pobierania aplikacji do śledzenia lokalizacji. Zastanawiali się, czy respondenci podejmowali niezbędne kroki w celu ochrony swojej prywatności. Sprawdzili, czy mają oni obawy dotyczące możliwego przyszłego

wykorzystania danych śledzenia kontaktów zebranych przez władze zdrowotne w Turcji i inne instytucje, takie jak np. Google.

Grupę respondentów stanowili użytkownicy smartfonów. Badania zostały zrealizowane za pomocą ankiety online z wykorzystaniem Formularzy Google. Ankieta składała się głównie z pytań narracyjnych. Respondenci byli proszeni o wyobrażenie sobie różnych scenariuszy, w których producenci aplikacji, operatorzy/producenci telefonów komórkowych lub rząd wykorzystywali niektóre ze swoich danych do badania lub łagodzenia rozprzestrzeniania się COVID-19. Następnie między 15 grudnia 2020 r. a 2 stycznia 2021 r. autorzy za pośrednictwem różnych sieci społecznościowych rozpowszechnili link do ankiety. Ankieta została przeprowadzona anonimowo. Analizie ilościowej poddano 444 kwestionariuszy ankiet.

Jak wskazują wyniki badań, poziom umiejętności cyfrowych badanych osób jest wysoki, co warunkuje wysoki poziom ich wykształcenia. Jednocześnie analiza odpowiedzi pokazała, że respondenci nie czytają warunków oferowanych w aplikacjach. Osoby dbające o prywatność wyraziły chęć udostępniania swoich danych w trosce o zdrowie publiczne. Przeprowadzone badania wykazały, iż wiedza ankietowanych na temat GCMR jest niewystarczająca. Respondenci byli niezdecydowani i zaniepokojeni tym, że w przyszłości władze wykorzystają ich dane z powodu niepewności doświadczanej w okresie pandemii.

Słowa kluczowe: COVID-19, Google Community Mobility Reports, umiejętności cyfrowe, prywatność cyfrowa, prywatność danych lokalizacyjnych, zmiany technologiczne

Smartphones are widely used among all age groups in Turkey. According to the state authorities, mobile subscribers reached 82.7m of the 83.6m total population in Turkey as of Q3 of 2020 and 64.5m of the total population are mobile Internet users (BTK, Information and Communication Technologies Authority 2020). They are technologically advanced tools that are equipped with powerful sensors and connectivity features. These sensors and features include Bluetooth capability, digital compass, accelerometer, GPS, Wi-fi, microphone, humidity sensors, health tracing sensors, cameras, etc. (Azad, Arshad, Akmal, Riaz, Abdullah, Imran, Ahmad 2020). In 2020, Google started to share the document named COVID-19 Community Mobility Report with users and governments using location data. The report evaluates the impact of COVID-19 on worldwide mobility with anonymized data received via Google Maps. It shows the movement trends according to geography over time in different categories such as retail and recreation areas, markets and pharmacies, parks, public transportation stations, workplaces, and housing (Google 2020). Google collects the location data of individuals, then processes, and shares them with the public favouring the idea that such reports will provide data support to policies developed to combat COVID-19.

It is widely argued that the location data used by governments and large global technology companies to prevent the virus may bring violations of surveillance, personal data security, and privacy (Leins, Culnane, Rubinstein 2020; Wen, Zhao, Lin, Xuan, Shroff 2020). Governments and researchers around the world are implementing digital contact tracing solutions to stem the spread of this infectious disease. On the other hand, contact tracing itself is not new – it is a well-established part of the response to any contagious disease outbreak (Fahey, Hino 2020). Although contact tracing is an essential tool for public health officials and local communities to fight the spread of novel diseases, such as the COVID-19 pandemic (Cho, Ippolito, Yu 2020), many of these solutions threaten individual rights and privacy (Berke, Bakker, Vepakomma, Larson, Pentland 2020). Apart from issues related to contact tracing apps, as people started to work from home or other places, weaker personal data security issues tended to increase. For example, it had been reported that the Zoom app was hacked and data of about 500K of users were affected in 2020 (Brough, Martin 2020; Mathews 13.04.2020).

Our aim is to find out whether individuals in Turkey are aware that their location and movement data are being tracked by Google Maps and the contact tracing apps for preventing the spread of the COVID-19. We also examined their motivations for downloading location tracing apps and whether they have been taking necessary steps to protect their privacy. We investigated whether they had concerns about the possible future use of contact tracing data collected by the health authorities in Turkey and other institutions like Google.

1. The COVID-19 global pandemic

COVID-19 spread rapidly all over the world after being reported for the first time in Wuhan, China in December 2019, (Ahn, Park, Lee, Hong 2020; Basellini, Alburez-Gutierrez, Fava, Perrotta, Bonetti, Camarda, Zagheni 2020). On January 30, 2020, the World Health Organization (WHO) declared a "Public Health Emergency of International Concern," and then a global pandemic on March 11, 2020 (WHO 16.02.2021). The total reported number of infections by WHO Regions as of February 16th, 2021 is just above 108.2 million with 2.4 million reported deaths worldwide. Turkey has reported 22 thousand deaths related to the COVID-19 and the numbers continue to rise (WHO 16.02.2021).

Due to the lack of an effective treatment method and the vaccine being so new, nearly all countries have adopted different restrictions such as travel bans, social distancing measures, mandatory mask use and various lockout methods to reduce the transmission of COVID-19 and minimize social contact (Basellini et al. 2020). Turkey, which had its first COVID-19 infection on March 11, 2020, according to the Turkish Ministry of Health (2021), has also enforced different measures like travelling limitations, curfew, online education and more to stop COVID-19 from spreading.

2. Surveillance through smartphone apps

Many governments in the world are using smartphone technology to digitally trace contact to prevent the spread of the disease. The Singapore government was the first in the world to launch a national Bluetooth contact tracing app on March 20, 2020 (Michael, Abbas 2020). There is an argument about whether mobile contact tracing architecture should be centralized in which all the detection is performed at a central server, or decentralized, in which each user (i.e., the smartphone) performs the detection. A decentralized one seems preferable because not every user encounter data, but only the diagnosed positive patient record is uploaded to the server. This method is also supported as an industry standard by Apple and Google (Wen et al. 2020). Decentralized contact tracing apps do not share users' information with a central authority but, nevertheless, have other privacy challenges (Bengio, Ippolito, Janda, Jarvie, Prud'homme, Rousseau, Yu 2020). The awareness and thoughts of individuals about these difficulties constitute the main subject of this study.

Surveillance is not a new issue and has not started with the COVID-19 Pandemic. According to Gwendolyn L. Gilbert, Chris Degeling, Jane Johnson (2019), for the reasons of "national security, crime prevention, road safety or public service improvement," states are constantly implementing surveillance methods. Surveillance takes place on citizens' data, when they move from one location to another, when they purchase something or when they spent their leisure time playing video games. These data are collected from many sources like internet searches, posts on social media, smartphone and tablet cameras, credit cards, and wearable devices. Most people are not aware that their data are collected and "anonymously" analyzed,

compared, integrated, and sold to the merchant ships as an old song said* (Gilbert et al. 2019).

As G.L. Gilbert et al. (2019) reported from Amy L. Fairchild, Ronald Bayer, James Colgrove (2007) and Lisa M. Lee, Charles M. Heilig, Angela White (2012); "Surveillance serves as the eyes of public health" or "the finger on the pulse of the health of a community." The WHO's definition of surveillance is as the "[…] systematic ongoing collection, collation and analysis of data for public health purposes and the timely dissemination of public health information for assessment and public health response as necessary" (WHO 16.02.2021). According to G.L. Gilbert et al. (2019), disease surveillance to combat and control the negative effects on society exists since the nineteenth century.

As the COVID-19 contact tracing apps collect, analyze and process sensitive information about individuals' health, location, name, age, e-mail, and nationality, it raises concerns about whether these data are properly treated by legal authorities or by the parties who collect them. Another concern is that if these data are further used after the pandemic and how. Because the apps allow the owners to track the users' visited locations and interactions on social media (Sharma, Bashir 2020). A recent study showed that contact tracing apps collect sensitive information (Wen et al. 2020). But despite its benefits in tracing and controlling the spread of the virus, publicizing contact trace data raises concerns about individuals' privacy (Jung, H. Lee, Kim, U. Lee 2020). This type of contact tracing has some other consequences. For example, local businesses can be ordered to close by local governments if visited by COVID-19 infected people (Dubov, Shoptaw 2020).

The decisions of governments and societies during the pandemic process, which can be considered the biggest crisis of our age, will also affect our future. Governments can always track everyone thanks to technology and will continue their surveillance practices by saying that "we are taking measures against the next virus even if the virus ends" (Harari 20.03.2020). With the COVID-19 surveillance, many researchers fear that history will repeat itself. Tanusree Sharma and Masooda Bashir (2020) think that in such times of fear and uncertainty, people will renounce their civil liberties, just as they did on September 11, 2001. Jessica Vitak and Michael Zimmer (2020) highlight that the temporary measures implemented after the terrorist attack in the USA became permanent and say that pandemic measures may likewise permanently

* See *Redemption Song* by Bob Marley from the album Uprising (https://en.wikipedia.org/wiki/Redemption_Song).

violate privacy. According to Ángel Díaz's interpretation (7.04.2020), the mass surveillance after the September 11 attacks provides a cautionary story for the COVID-19 pandemic. Such ideas seem very dystopian for now, as the technology and digital literacy of people in 2001 are quite different from the current world. While personal information could easily be collected in the period of September 11, anonymous collective data is generally used now.

3. Contact tracing and privacy dilemma during the COVID-19 pandemic

Although there are undeniable benefits in the containment of the COVID-19 virus, collecting data about the contact histories of people who installed contact tracing apps raises concerns about individuals' privacy (Jung et al. 2020). There is an ongoing discussion about the perils of the effective use of these automated technologies and the danger they bring to the privacy and security of individuals (Simko, Calo, Roesner, Kohno 2020; Sun, Wang, Xue, Tyson, Camtepe, Ranasinghe 2020; Wen et al. 2020).

For contact tracing, it is important to locate people when they are within 1.5m to 2m of an infected person for at least 10 to 15 minutes. More importantly, for such a contagious disease, fast contact tracing is not possible manually (Abeler, Bäcker, Buermeyer, Zillessen 2020). Muhammad Ajmal Azad et al. (2020) argue that "a protocol for contact tracing" is necessary to ensure the proper use of the private data of individuals. This protocol should provide a "consent mechanism" because such apps usually collect data without informing the users. Privacy-literate users may prefer not to share their data. But such behaviour may hamper preventive efforts that governments may have made (Azad et al. 2020). On the other hand, when the number of cases increases as the virus spread all over the world, contact tracing becomes difficult to operate (Cho et al. 2020).

There are some privacy concerns that we seek to find answers to in our research mentioned in a paper by J. Vitak and M. Zimmer (2020). According to the authors, the questions of "who can access data," "how long is data stored," and "for what purposes could that data be used in the future" are the biggest concerns of this pandemic.

Aex Dubov and Steven Shoptaw (2020) argue that there are ethical issues in using contact tracing technology since the success of this technology depends on "people's willingness to participate" and any compulsory measure

may face resistance. To maintain participating and allowing the authorities to contact tracing, voluntariness is essential in deciding to download and share personal information through the app. According to Aaron R. Brough and Kelly D. Martin (2020) "widespread adoption of new surveillance tools to monitor and prevent contagion" has caused weaker protection of data and individuals lost control of their personal information, which they called "eroded privacy." Further, they argue that such surveillance has forced some people to replace offline activities with online activities.

From an ethical point of view, since adopting massive digital surveillance throughout the world is essential to protect the lives of millions of people, what becomes important for governing authorities is that the policies to combat this disease must consider protecting sensitive data being collected and analyzed and processed. In other words, they must maintain transparency without potential loss of privacy. This is one of the major concerns about privacy rights and civil liberties (Sharma, Bashir 2020).

The containment strategies may cause a negative effect on identifying the COVID-19 positive patients. When they are publicly identified, they may be at risk and face harsh treatment by others in the community. For example, in China, individuals use an app to identify symptoms of the disease and report them to the police (Raskar, Schunemann, Barbar, Vilcans, Gray, Vepakomma, Werner 2020). Similarly, a contact tracing app in Turkey, called Hayat Eve Sığar [n.d.] (HES-Life Fits into Home) has a "report a violation" function to take pictures of the one who is violating the social distancing and self-isolation rules and send them to the authorities.

As the novel COVID-19 is very contagious, to stop spreading needs rapid containment strategies to be applied by governments all around the world. Determining the location and contact history of infected individuals is the priority. The ubiquitous use of smartphones is an advantage, but it has the risk of massive surveillance by exposing private information about people (Raskar et al. 2020). As A. De Carli, M. Franco, A. Gassmann, C. Killer, B. Rodrigues, E. Scheid, D. Schoenbaechler, B. Stiller (2020) and Marcello Ienca and Effy Vayena (2020) comment that if contact tracing apps use these data and algorithms in a responsible manner and be privacy-sensitive, then we can achieve a democratic and open world without sacrificing public trust. Similar tracing apps notifying authorities when patients in quarantine leave their homes are available in Iran and South Korea as well (Raskar et al. 2020).

But it is difficult to achieve the goal of having privacy-sensitive apps. Because, according to Alex Berke et al. (2020), even if these apps anonymize user

data, it is possible to match these data with very few secondary data records to have more information about users. We see a dichotomy in the COVID-19 contact tracing app policy. Priorities of governments around the world differ slightly. One approach is the "privacy-first" which aims to protect user data. On the other end, the "data-first" approach aims to store and benefit user data as much as possible to fight the virus (Fahey, Hino 2020). For example, governments in China, South Korea, Israel, and elsewhere have a data-first approach and openly accessed and used personal data for tracing purposes. On the other hand, particularly in Europe, both national and regional laws enforced a more privacy-focused approach by adhering to the General Data Protection Regulation. The GDPR, which was published on May 4, 2016, became effective on May 25, 2018, thereby placing limitations on such tracing activities (Intersoft Consulting, 2016; Oliver, Lepri, Sterly, Lambiotte, Deletaille, De Nadai, Vinck 2020). The lack of consensus over the use of contact tracing app data among the nations may create some problems including intrusions on citizens' privacy and challenge the use of "large-scale public data." People are more sensitive and conscious about their private data and this has not started with the COVID-19 pandemic. It has roots back in Facebook-Cambridge Analytica Scandal in the 2016 US Presidential Elections (Fahey, Hino 2020). Therefore, to protect the democratic climate, it is important to know that although people are aware that some tracing activities are necessary to control and prevent the disease. But there are concerns, specially voiced by human rights siders that this surveillance to be prolonged after the disease ends (Oliver et al. 2020).

4. Permission requirement and what data contact tracing apps collect

Mobile technologies, in general, aim to make our lives easier, more productive, and healthy by collecting various types of personal data, including location and movement data as well as social media content. Users have little understanding of how their data is processed and used for what purposes (Vitak, Zimmer 2020). Muhammad Ajmal Azad et al. (2020) found in their research that most of the apps collect personal data including name, phone number and location. They suggest that giving the user the power to select among a list of permissions may help to achieve the transparency they want. Marcello Ienca and E. Vayena (2020) also point out the same suggesting transparency in public communication about data access and use.

During the pandemic period, individuals became so sensitive about the protection of personal data that the news that WhatsApp updated its terms and privacy principles in the first weeks of January 2021, that we mostly approve without reading while subscribing to the applications, causing a great reaction. Tens of thousands in Turkey used the #WhatsAppSiliyoruz (#deleteWhatsApp) hashtag in their tweets on Twitter. According to the news from BBC, Facebook postponed their new regulation after this reaction (BBC News Turkey 16.01.2021).

5. Google and Apple cooperation

When we consider how it started, this quotation from Katina Michael and Roba Abbas (2020) is quite remarkable:

> Invited into the early discussions in the White House to help with a response to coronavirus, it became apparent in the US that the President was requesting the support and expertise of the largest technology firms in the Western world. Ten days before Singapore launched TraceTogether, representatives of Google, Amazon, Facebook, Apple, Microsoft, and Twitter were already meeting with the US chief technology officer, Michael Kratsios, on March 10, 2020.13 Each had a role to play: Amazon would make sure predatory selling by third parties on its platform would be eradicated, Twitter would minimize the amount of "fake news" being propagated on its platform, and Google could generate location reports to demonstrate how states were keeping to self-isolation orders. But what of the possibility to offer contact tracing? This seemed like the perfect opportunity for America's biggest companies to come together in a show of solidarity–Google and Apple could join forces on the development of the contact tracing app, Amazon and Microsoft could offer storage and web services, and Facebook and Twitter could cover social media matters.

Google and Apple are the most prominent technology companies in the world. They are supposedly supporting most of the data traffic in the world through their internet servers, operating systems, application stores, smartphones and Internet of Things (IoT) devices (Romm, Harwell, Dwoskin, Timberg 10.04.2020). Google and Apple cooperation is one of the most notable technological partnerships in the COVID-19 pandemic. This tool is widely accepted by privacy siders because it ensures data privacy and

security since it has a decentralized approach thanks to Bluetooth technology (Azad et al. 2020; Whittaker 20.04.2020).

Jessica Vitak and M. Zimmer (2020) also point out that "Google/Apple have resisted pressure from governments who want access to app data to build a picture of population movements in aggregate" and answered users' expectations about data privacy. On the other hand, after the mob attack on the US Capitol by Trump supporters (Borger 7.01.2021), we saw that Google (Youtube) and Twitter, along with other social media platforms like Facebook and TikTok, restricted/suspended Trump's accounts, preventing him from posting messages. These "authoritarian acts" are questionable in terms of democratic principles and human rights. After Twitter's ban on Trump's account, Jack Dorsey needed to explain their action to the public (Phillips, Ellis-Petersen, Walker, Wong 17.01.2021). Another concern spoken by K. Michael and R. Abbas (2020), regarding the power these technology companies acquiring is that "[for] example, will Google's FitBit work hand in hand with Android devices gathering 250 000 points a day per user and will other more innovative systems be introduced down the track once the pandemic is over to help us rise to the challenges of the Fourth Industrial Revolution?" On the one hand, the decentralized approach of Google/Apple cooperation has positive returns in terms of human rights. But on the other hand, as these big tech companies have enormous power and control over social media, authoritarian acts may produce negative returns in terms of data privacy.

6. The preventive efforts of Europe and other nations

In Europe, governments are taking some measures to protect the privacy of data. According to European Union's General Data Protection Regulation, categories of normally protected information such as genetic data, political and religious affiliations, and criminal history can be freely shared in crisis situations (Brough, Martin 2020). Tanusree Sharma and M. Bashir (2020) point out that The European Data Protection Board issued a statement emphasising the importance of protecting personal data while fighting COVID-19. Since it is about processing personal data, this statement is important. The Article 9 mainly states that personal data can be processed in favour of the public interest, proportionately to the intended aim of protecting public health and respecting the rights and freedoms of individuals (Ienca, Vayena 2020).

To combat COVID-19, all nations and their authorities are implementing measures benefiting from technology, especially smartphones, street cameras, thermal cameras, and facial recognition software to identify risky individuals and track their location (Singer, Sang-Hun 24.03.2020). The first country to start using Bluetooth-enabled tracing app was Singapore in March 2020 (Michael, Abbas 2020). India and the United Kingdom use "smart city" technologies. Israel uses tracing technologies to detect user's smartphone data, tracing movements, contacts and "interpersonal interactions." Especially in the United States, where the highest death toll was achieved, Google and Apple partnered for contact tracing using smartphones. And in China, a backlash was caused due to an unexplained system that determines people's contagion risk as red, green, or yellow, even when using public transportation (Abeler et al. 2020; Brough, Martin 2020; Singer, Sang--Hun 24.03.2020). Many countries including Germany, Austria, Switzerland, Estonia, and the Czech Republic, with possible flips by Australia, the UK, New Zealand, and France preferred Google/Apple app technology, instead of using domestic apps (Michael, Abbas 2020). Haohuang Wen et al. (2020) explain that in Turkey, the government-owned HES App stores "the current user's ID in a readable characteristic." These fixed ID scans be accessed by a nearby smartphone connected and can track the user. With this ID data, one can track the user when moving around different locations.

When we consider different approaches taken by different nations, we can highlight that there is not only one solution to the problem of tracing individuals while maintaining their privacy. As Md Whaiduzzaman, Md. Razon Hossain, Ahmedur Rahman Shovon, Shanto Roy, Aron Laszka, Rajkumar Buyya, Alistair Barros (2020) posit that using tracing apps should be a "voluntary act" and the authorities or any third party should "not mandate users to use these apps in any circumstances." In this regard, Kelly D. Martin, Abhishek Borah, Robert W. Palmatier (2017) and A.R. Brough and K.D. Martin (2020) suggest that "providing transparency" and "allowing consumers to control how their data will be used" have positive effects.

7. Social distancing and geolocation

Social distancing has been the most important preventive strategy to combat the spread of COVID-19. It is argued that to get back to regular social and

economic activities, health authorities like WHO and governments especially insist on applying social distancing rules very carefully. These rules are essential "to crowd-source information concerning the health of individuals" and "to ensure that social distancing rules are being respected" (Carli et al. 2020). Lucy Simko et al. (2020) point out that to understand the effect of social distancing, several companies have benefited from geolocation data immobility.

An interesting finding about the implementation of the restrictions is that generally Asian countries have applied the "strict and punishable rules on social distancing." On the other hand, the European countries have preferred the "recommending people to stay at home" approach and kept privacy and individual freedom untouched (Huynh 2020).

An interesting finding about the effect of social distancing and isolation in Chiou and Tucker's work as mentioned in a paper by Xiao Huang, Zhenlong Li, Yuqin Jiang, Xinyue Ye, Chengbin Deng, Jiajia Zhang, Xiaoming Li (2020) points out that people with high earnings are more likely to comply with the social distancing regulations.

South Korea's method of social distancing and contact tracing application deserves a detailed investigation. Because the country did not impose lockdowns and business closures that other countries have implemented. Instead, they made massive COVID-19 testing and effective contact tracing program. It is done by collecting location data of positively tested people. Instead of matching location data from infected people within the population, the government officials preferred to "anonymize" and publish the location data of the patients on websites for everyone on a daily basis. This is remarkably similar to the Google COVID-19 Community Mobility Report. On the other hand, Jay Stanley and Stisa Granick (2020) mention a study that "just knowing the zip code of where you live and where you work will uniquely identify 5 per cent of the population." When identifying a person is that much easy, being and staying anonymous become a big problem. Therefore, identified location data can have the potential to reveal other sensitive information like "people's social, sexual, religious, and political associations."

8. Google Community Mobility Reports

The spread of infectious diseases is much faster, especially considering the mobility of millions of people in our globalising world. As M. Ienca and

E. Vayena (2020) say, COVID-19 has occurred in a much more digitalized and connected world than previous global virus outbreaks. Cell phone data (especially location data) collected from users are used by most governments and large technology companies to measure human mobility and control the spread of COVID-19.

Social distance and curfews, which are important measures for countries trying to control the pandemic, are economically expensive. For this reason, most countries have evaluated digital applications offered by major technology companies to minimize contact. Gabriela Cavalcante de Silva, Sabrina Oliveira, Elizabeth F. Wanner, BLeonardo C.T. Bezerra (2020) explain that Google has offered anonymous mobility data of users free of charge for many countries including Turkey to track social distancing. The GCMR, covering more than 130 countries, is a good example of how tech companies are helping to combat COVID-19. Google hopes that by bringing this study to the public, it will aid critical decisions in dealing with the virus (Dogan 2020). "These Community Mobility Reports aim to provide insights into what has changed in response to policies aimed at combating COVID-19" (Google 2020).

There are different place categories in the report such as "retail and recreation places," "markets and pharmacies," "parks," "public transport stations," and "workplaces and residences" (Google 2020). The Community Mobility Report, first published by Google in March 2020, is based on anonymous aggregated location data from users who have turned on their location history setting (turned off by default in their Google account; Silva et al. 2020). Google says to protect the privacy of its users, personally identifiable information such as location, people and movements will never be used. It also states that users with open location history can turn this setting off at any time and delete their data from their timelines (Google 2020). Google frequently emphasizes the importance it attaches to user privacy and security in its report, which is composed of anonymous data sets, and states that this report is only intended to help fight the COVID-19 outbreak. In addition, Google stresses that these data will never be used after the pandemic.

The GCMR use aggregated, anonymized datasets to graph movement trends by geography and location categories and show occupancy of specific location types. Public health officials have suggested that the use of these data in the fight against COVID-19 can be particularly useful in making critical decisions (Aktay, Bavadekar, Cossoul, Davis, Desfontaines, Wilson 2020). Google has generated the mobility data it provides by comparing visits to certain locations and duration of stay using location data collected from Google

Maps (Yilmazkuday 2021). Google compares the changes during each day with a reference value for that day of the week. The reference day is the median value for the 5-week period between January 3rd and February 6th, 2020 (Barrios, Benmelech, Hochberg, Sapienza, Zingales 2021; Google 2020).

The GCMR reveals the differences in mobility with different location categories in the pre- and post-pandemic periods. In terms of efforts to reduce COVID-19, this report could help combat the pandemic. It can also reveal to what extent measures such as lockdowns and contact tracing work in different regions (Saha, Barman, Chouhan 2020). The GCMR also provided data for most scientific studies conducted during the pandemic period. Using the data provided by Google in its report; Michał Wielechowski, Katarzyna Czech, Łukasz Grzęda (2020) were able to identify changes in mobility in public transport during the pandemic process; Hakan Yilmazkuday (2021) investigated the causal relationship between country-specific changes in mobility and the number of COVID-19 cases and deaths; Ugofilippo Basellini et al. (2020) examined the relationship between human mobility and excessive deaths; Cristina M. Herren, Tenley K. Brownwright, Erin Y. Liu, Nisrine El Amiri, Maimuna S. Majumder (2020) showed that the decrease in mobility can be explained by the degree of economic development and democracy in countries.

Although the GCMR has created a useful dataset to understand the mobility of the pandemic process, choosing January 3rd – February 6th, 2020 as a reference interval can be misleading. This is because there is a differentiation in the mobility of people between January and June, regardless of the pandemic. For example, people who usually stay at home due to the weather during the winter months will move more in the summer.

Examining Google reports on mobility data in Turkey between March 11, 2020, and January 20, 2021, Figure 1 shows that the highest mobility in the "retail and recreation" category was on August 4, 2020 (1.445%), and the lowest on January 1, 2021 (-28.740%). The mobility of the "market and pharmacies" category appears to be the highest on May 22, 2020 (21.126%), and the lowest on April 11, 2020 (-22.980%). The mobility in the "Parks" category appears to be the highest on August 2, 2020 (24.903%) and the lowest on January 3, 2021 (-25.167%). It is observed that the mobility of the "public transport stations" category is the highest on 30 July, 2020 (8.835%) and the lowest on December 5, 2020 (-20.849%). The mobility in the "workplaces" category appears to be the highest on July 26, 2020 (2.709%) and the lowest on January 1, 2021 (-42.634%). It is observed that the mobility of the "housing" category is the highest on January 1, 2021 (12.702%) and the lowest on August 2, 2020 (-1.597%). According

to anonymous data in the report, community mobility in Turkey has decreased during the pandemic period. It strikingly shows the lowest mobility data for the "retail and recreation" and "workplaces" categories on January 1, 2021, while also showing the highest data for the "residential" category. This is due to the intense security measures taken by the state to prevent the New Year celebrations. Looking at the total data of the report, the percentage of movement in crowded areas has decreased significantly. The biggest reason for the decline in the categories of "retail, recreation" and "workplaces" categories is the government bans and the transition of most of the workplaces to the home working system. Again, from the same perspective, the reason for the rise in the "housing" category is the stay-at-home restrictions.

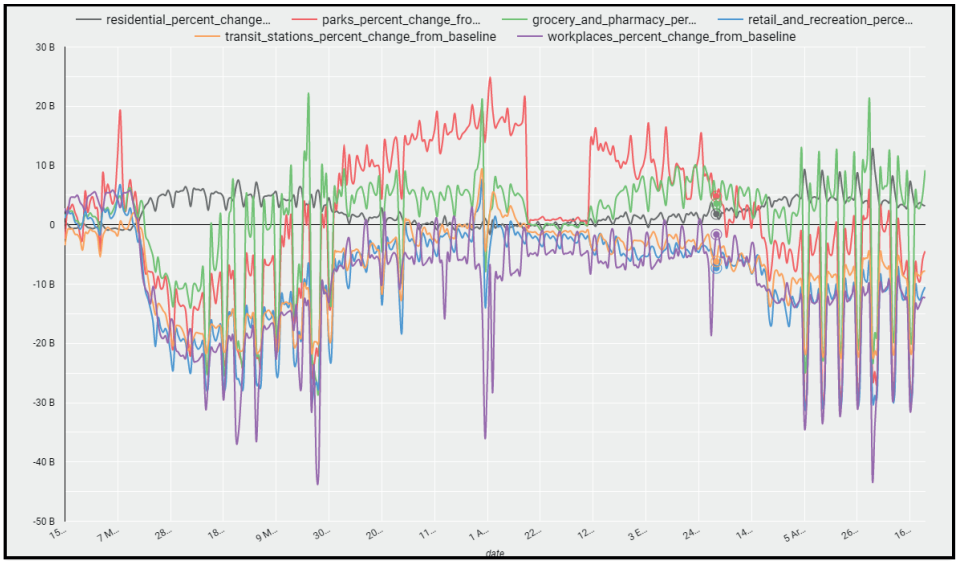

Figure 1. COVID-19 – Google Global Mobility Reports

Note. Data is constantly updated directly from Google. Mobility data is shown for Turkey only.
Source: COVID-19 – Google Mobility Report (2020).

9. Economic and social impact of the pandemic

The Coronavirus Disease 2019 will drastically change the global economy as it reduces daily activity and therefore limits business activity (Hussein, Shams, Apu, Rahman, Mamun 2020). In this gloomy period of the economy,

politicians had to choose between saving the lives of millions and saving the economy (Coibion, Gorodnichenko, Weber 2020). Governments temporarily locking down cities to contain the pandemic can reduce the productivity of individuals as well as limit transport operations, affecting the market and causing strong economic losses (Raskar et al. 2020; Wang, Yamamoto 2020; Whaiduzzaman et al. 2020). A restriction has enormous costs for both employers and workers. For this reason, most countries have gradually lifted the quarantine with the decrease in the number of cases in order to mitigate the economic impact of the epidemic. However, the latest epidemiological models predict that lifting the restrictions will cause the epidemic to restart (Basellini et al. 2020; Ferguson, Laydon, Nedjati Gilani, Imai, Ainslie, Baguelin, Ghani 2020). The economic impact caused by the COVID-19 pandemic that transformed the world has not yet been fully determined, but from a historical perspective, it is predicted to have a major impact as it did during the Great Depression (1929–1933) period (Barro, Ursúa, Weng 2020; Gvili 2020; Laing 2020; Wielechowski et al. 2020). With the rising number of cases due to the secondary COVID-19 outbreak, how countries will save the economy is, unfortunately, a question that has not yet been answered as the spread of virus mutations began in 2021 (Nature 4.02.2021; Roberts 3.02.2021).

Contact tracing practices offered by large companies can prevent the economic downturn brought about by lockdowns. According to K. Michael and R. Abbas (2020), the value proposition of contact tracing practices eased lockdown measures and brought local economies back to work. Looking from another perspective, as Naomi Klein (13.05.2020) said, while COVID-19 kills thousands, large tech companies that have become monopolized are taking the opportunity to expand their power and amount of data. Even though the applications offered by technology giants such as Google and Apple seem to be of public interest during the difficult pandemic period, there is no guarantee that this data will not be used to our disadvantage or sold to governments for the sake of further surveillance.

Another shortcoming of the economic consequences of the COVID-19 crisis is that low-income households have lower-quality technological devices. This will lead to difficulties in using applications developed to prevent the pandemic and less opportunity to develop digital literacy skills (Beaunoyer, Dupéré, Guitton 2020) Contact tracing applications developed by governments and application manufacturers should be available and accessible to everyone. If certain demographic groups have difficulty accessing these applications, the effectiveness of contact tracing applications will decrease (Simko et al. 2020).

Equality and social justice in contact tracing practices are not always possible for all countries and people. People with low income may have difficulty accessing a smartphone, and people who do not have digital literacy may not be able to use these applications (Raskar et al. 2020). The most vulnerable groups in the use of mobile apps are the elderly, the homeless and low-income families. Application developers should consider these disadvantaged groups and come up with solutions accordingly. Limited access to technology can be vital for users during the pandemic period (Dubov, Shoptaw 2020). Additionally, people who are not digitally literate may not be aware of the risks associated with privacy and are therefore vulnerable to data breaches during the COVID-19 period (Anderson, Heesterbeek, Klinkenberg, Hollingsworth 2020).

The increasing use of technology in the COVID-19 pandemic has brought the already existing digital divide to the surface (Beaunoyer et al. 2020; Buchholz, DeHart, Moorman 2020). When population-level inferences are made from the data of people with access to technology, the analysis created over specific populations will mislead the policy, as the remaining disadvantaged groups cannot be included in the reports (Chunara, Cook 2020). People who are not included in the reports will also be lagging in the developments related to the virus, as they do not have the chance to review the reports. Because of these reasons, as Beth A. Buchholz et al. (2020) mention, every citizen must be digitally-literate and access the latest technology available for people of all ages to follow up-to-date information and to connect with their environment during quarantine periods. Digital literacy training should be provided to individuals to enable them to transition to digital citizenship. As Yuval Noah Harari (20.03.2020) stated, we must prepare ourselves for what kind of world we will live in after the pandemic crisis. Digital tracing applications, which are now actively used almost all over the world, may cause great problems in the future. To cope with these challenges, people should be open to transformation and focus on digital literacy education.

10. Purpose of the present study

This study aims to measure individuals' awareness, priorities, and privacy degrees on the use of their data in the COVID-19 pandemic. We aimed to measure the privacy values, concerns, and thoughts of the participants about contact tracing applications during the pandemic. In this study, we provide a summary

of the participants' views on potential contact tracing scenarios. Because as L. Simko et al. (2020) mention, many countries implemented contact tracing applications during the pandemic, and it has socioeconomic effects on society.

We have four main questions (hypotheses) in the research as shown in Figure 2: First, what is the level of digital literacy of individuals? Second, what are the opinions of individuals regarding the use of location data by different sources to study or mitigate the spread of COVID-19? Third, what are individuals' views on Google Community Mobility Reports (GCMR), which is a helpful tool for health authorities as they make critical decisions to combat COVID-19? Finally, did individuals download the HES application, and if so, what are their motivations?

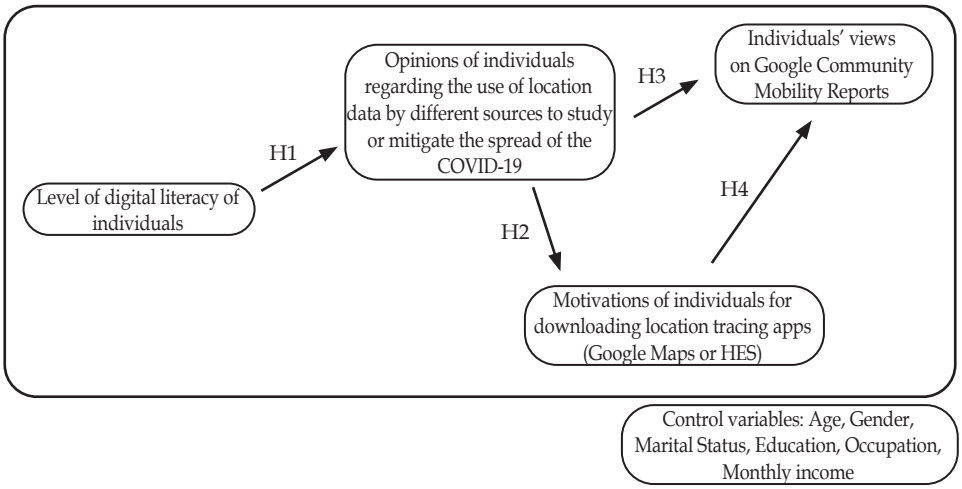

Figure 2. The Research Model

Source: own study.

11. Method

11.1. Sample

We reached 444 people with the online survey method in the study we conducted to measure the digital literacy levels, awareness, and privacy concerns of individuals during the COVID-19 period. Then we eliminated a total of 2 invalid questionnaires.

We asked six demographic questions to participants: age, gender, marital status, education level, employment status, and monthly income. When we examine the demographic characteristics presented in Table 1, it is seen that most of our participants are between the ages of 25–34 (43.9%), the sample is mostly female (61.3%) and more than half of the participants are single (n_f = 257/442). According to the results of the survey, most of the participants have a high level of education and most of them are undergraduate, graduate, and doctoral degrees (81.9%). While 65.2% of the participants are working, 25.3% are students or unemployed / looking for jobs. A monthly income of more than half (57.3%) is between 2.501 TL–5.000 TL and 5.001 TL–10.000 TL.

Table 1. Demographic Information of the Sample

Demographic Information	Categories	Frequency	Percentage
Age	≤17 y	10	2.3
	18–24 y	62	14.0
	25–34 y	194	43.9
	35–44 y	81	18.3
	45–64 y	85	19.2
	≥65 y	10	2.3
Gender	Female	271	61.3
	Male	171	38.7
Marital Status	Married	185	41.9
	Single	257	58.1
Education	≤ High school graduate	56	12.7
	Associate degree	24	5.4
	Bachelor's degree	192	43.4
	Master's degree	99	22.4
	Doctorate degree	71	16.1
Occupation	Employed	288	65.2
	Retired	42	9.5
	Student	61	13.8
	Unemployed	51	11.5
Monthly income	≤1.500₺	66	14.9
	1.501–2.500₺	31	7.0
	2.501–5.000₺	109	24.7
	5.001–10.000₺	144	32.6
	10.001–14.999₺	48	10.9
	≥15.000₺	44	10.0

Source: own study.

11.2. Instrument

To collect the data we needed to design an online survey with 29 multiple-choice questions that take about 10 minutes. The survey was inspired by *COVID-19 Contact Tracing and Privacy: Studying Opinion and Preferences* written by L. Simko et al. (2020) and was redesigned for our research. Our survey consists mostly of narrative questions, where we asked respondents to imagine various scenarios where app manufacturers, mobile phone operators/manufacturers, or the government were using some of their data to study or mitigate the spread of COVID-19. In the survey, eight main parts were explained in detail in *Descriptive statistics*. Only participants who knew about the GCMR report could see the survey section for GCMR.

Instead of directly asking about privacy or confidentiality, to avoid prompting participants with questions, we asked about their comfort level in specific situations or the possibility of downloading an app. In the questionnaire, which consisted of Likert scale questions, apart from demographic questions and questions with checkboxes, the participants were asked to rate each question as *poor* (1), *fair* (2), *indifferent* (3), *very good* (4), or *excellent* (5) in response to each question. These ratings were adapted for each question depending on the question. For example, in some questions the options were *I definitely would not* (1), *I would not* (2), *I am indecisive* (3), *I would* (4), *I definitely would* (5).

11.3. Design

We used a quantitative research design in our study. At first, we tested the online survey we created on Google Forms with 15 people who have similar demographic characteristics and completed our pilot study. Then we distributed the survey link to the participants through various social network sites (Twitter, LinkedIn, WhatsApp, Facebook) between December 15, 2020, and January 2, 2021. We analyzed the data of 444 people, collected anonymously, with IBM SPSS Software.

When we look at the limitations of the research, we disseminated the questionnaire online due to COVID-19 and used only social media in announcing the survey. The majority of the participants were highly educated and between the ages of 25–34. This situation caused difficulties in interpreting the survey data. Besides, since we spread the questionnaire online, we were able to reach participants who already had a certain level of digital literacy.

11.4. Results

11.4.1. Descriptive statistics

Are you digitally literate? In this question category, we asked four questions to learn the level of digital literacy of the participants. First, we asked if they knew the privacy settings of the applications installed on their phones, and 65.4% said they did. In the next question, we asked if they knew how to change their location permissions on these applications and 76.6% said they did. Also, we asked the participants whether they read the terms and conditions offered while installing the applications on their phones or when signing up, and 78.3% said they did not. Finally, we asked which of the personal data they think the Google Maps app on their phones can access/the current location data (93.4%), e-mail (55.4%), name (60.4%), home address (70.8%), phone/device type (65.4%), current business/employer (48.4%) and hobbies (23.5%).

COVID-19 degree of anxiety and importance of social distance. We asked participants how worried they were about COVID-19 and 66.9% said they were worried. In another question, we asked if they believed social distancing is an important tool to slow the spread of COVID-19, and 95.7% said they did.

Google Community Mobility Reports questions. We asked participants about Google Mobility Reports in this question category. In the first question which was based on location categories in the data announced by Google, we asked the participants' frequency of being in these locations during the pandemic. When we examine the percentages in Table 2, we observe that participants seldom go to the retail and recreation category (79.0%), sometimes go to grocery and pharmacy (41.0%), few go to parks (65.6%), most never use public transport (83.0%). We concluded that more than half of them do not go to work (56.6%) and almost all of them are in their homes (92.1%).

Table 2. The frequency of being in places (GCMR Categories) in Turkey (December 15, 2020, and January 2, 2021)

GCMR Categories	Never/Rarely	Sometimes	Often/Always
Retail and Recreation	79.0%	18.3%	2.7%
Grocery and Pharmacy	39.1%	41.0%	19.97%
Parks	65.6%	17.6%	16.7%

Transit Stations	83.0%	10.4%	6.6%
Workplaces	56.6%	13.1%	30.3%
Residential	2.9%	5.0%	92.1%

Source: own study.

When we asked respondents if they knew about the GCMR produced using location data to measure community movements and slow the spread of COVID-19, the majority said they did not (80.8%). After this stage, we asked questions about GCMR only to participants who knew the report. The first question we asked the participants who knew the report was their opinion on whether the report would be really useful in preventing the spread of the virus, and more than half of them (68.0%, n = 85) said they thought it would be useful. In the other question, we asked whether they would like to share their data for public health if Google said in this report that it would use participants' data and not anonymized location data. Participants could not give a clear answer to this question, as 37.6% said they would not want it, 23.5% would be undecided, 38.9% would be willing to share. Finally, we asked the respondents if they considered the report to give importance to confidentiality, and the overall respondents (48.2%) said they were undecided, while the remaining majority (35.3%) thought they did not.

Questions about cell phone applications. We asked five questions to measure participants' comfort levels and privacy limits about an imaginary application that collects user data to study and mitigates the spreading of COVID-19. In the first question, participants had to choose at least one of the following permissions to be able to use the application after downloading it; permission to access the calendar, permission to access the camera, permission to access the directory, access to location information, access to phone features. We asked if they should grant at least one of the options. Out of 442 participants, 56.1% would not allow a calendar, 96.6% would not allow the camera, 94.3% would not allow a phonebook, 39.4% would not allow location information, 90.7% would not allow phone features, 95.0% would not allow microphone, 96.4% stated that they would not allow messages, 95.5% would not allow storage/recording settings, and 97.5% would not allow photo gallery.

In the next question, we let them suppose that the developers of the imaginary application will always know the locations of the participants but

will never share them with anyone. When we asked the participants if they would use this application, 36.4% said they would never use it, 22.4% were indecisive and 41.2% would use it. In the third question, we let them imagine that the application was produced by different organizations and asked them to evaluate how comfortable they would be with this application. According to the answers of the participants; 41.9% would be comfortable with the Turkish Ministry of Health (HES), 45.9% would be comfortable with the WHO, 34.8% would be comfortable with a university research group, 46.2% would be uncomfortable with Google (Google Maps), 47.5% would be uncomfortable with Apple (Apple Maps), 51.6% would be uncomfortable with Yandex (Yandex Navigation), 46.2% would be uncomfortable with an activist group, 51.8% would be uncomfortable with an entrepreneurial technology company. In another question, the developers of the imaginary application would know the participants' locations and when the participants' COVID-19 tests were positive, the manufacturers of the application would share location data with the government. In such a scenario, 45.7% of the participants said they would not use this application. About half of the respondents (55.2%) said that if the app developers shared their location data publicly, they would not use the app.

Questions about cell phone manufacturers and operators. We asked respondents how comfortable they would be if mobile phone operators/manufacturers would use participants' location data to study or mitigate the spread of the COVID-19, and 49.5% said they would be uncomfortable. In another question, we asked how comfortable the participants would be if mobile phone operators/manufacturers would share their data with the government for the same reason and 62.4% said they would be uncomfortable. Under the same conditions, we asked participants how comfortable they would be if mobile phone operators/manufacturers would share their location data with the government if their COVID-19 tests were positive, and 42.1% said they would be uncomfortable, 42.5% said they would be comfortable. In the last question, we asked participants how comfortable they would be if mobile phone operators/manufacturers would share their location data publicly if their COVID-19 tests were positive, and 63.1% said they would be uncomfortable.

Sharing location data with the government. We asked participants to suppose that the government received location data or contact data directly from an app on their phone or from mobile phone operators to study or mitigate COVID-19. In our question, we asked them to consider that

location data would only be shared with government public health officials, hospitals, and local law enforcement agencies, and how comfortable they would be if they had access to their location data. 46.4% said they would be comfortable with public health officials, 49.3% would be comfortable with hospitals, and 47.7% would be uncomfortable with local law enforcement. In our other government question, we asked how comfortable participants would be if their location data were shared with the government before the first known cases of COVID-19 i.e. before March 2020. The vast majority (76.9%) said it would be uncomfortable.

Why did you download the HES app? We asked the participants if they downloaded the HES app proposed by the Ministry of Health in Turkey to study or mitigate the spread of COVID-19 and 76.5% said that they did download it. We asked those who downloaded the app about the reason and 15.6% said to get on urban public transport, 56.3% said to see the local density of cases around them, 5.4% said because they were infected by COVID-19, 29.0% said because they wondered how the application works, 37.6% said they downloaded it to enter government buildings and 29.6% for intercity or inter-country travel.

After the COVID-19. We asked respondents if they expected app makers or phone operators/producers to stop storing location data after the pandemic was over and 51.8% were expecting it. Likewise, we asked how likely they thought the government was to delete data collected on their smartphones after the pandemic was over, and 67.4% said it was very unlikely. Finally, we asked participants if they were considering deleting applications that use location data from their smartphones to reduce or examine the spread of COVID-19 after the pandemic, and 79.9% answered yes.

11.4.2. Inferential statistics

A significant relationship has been determined by using Fisher's Exact test between knowing the privacy settings on the phone and gender (Chi-Square = 7,334; p = 0,004). There is no significant relationship between knowing how to change location permissions on the phone and gender (Chi-Square = 1,366; p = 0,147). There is no significant relationship between reading the contracts of applications installed on the phone and gender (Chi-Square = 0,194; p = 0,372).

According to the Mann-Whitney U test, there is a significant difference between age groups in terms of knowledge of privacy settings (U = 19206; p = 0,017). There is a significant difference between age groups in terms of knowing how to change location permissions on the phone (U = 8997;

p = 0,000). There is no significant difference between age groups in terms of reading the contracts of applications installed on the phone (U = 15856; p = 0,474). There is no significant difference between education levels in terms of knowledge of privacy settings (U = 21272; p = 0,491). But there is a significant difference between education levels in terms of knowing how to change location permissions on the phone (U = 12386; p = 0,001). There is no significant difference between education levels in terms of reading the contracts of applications installed on the phone (U = 15263; p = 0,201). There is no significant difference between education levels in terms of knowing the GCMR (U = 13637; p = 0,127). There is no significant difference between gender in terms of concerns about COVID-19 (U = 21124; p = 0,100).

A significant relationship between knowing the privacy settings on the phone and knowing how to change location permissions on the phone has been determined by Fisher's Exact test (Chi-Square = 83,691; p = 0,000).

According to the Mann-Whitney U test, there is no significant difference in COVID-19 anxiety between those who believe that social distance is an important tool and those who do not (U = 32225; p = 0,126). There is a significant difference between those who believe that social distance is an important tool and those who do not in terms of taking public transport (U = 32225; p = 0,126).

According to Spearman's Correlation test, there is a significant negative correlation between the COVID-19 anxiety and visiting retail and recreation stores (rho = -0,153; p = 0,001). There is a significant negative correlation between COVID-19 anxiety and visiting parks (rho = -0,097; p = 0,042). There is a significant correlation between COVID-19 anxiety and staying at residencies (rho = 0,293; p = 0,000). There is a significant negative correlation between taking public transport and income level (rho = -0,233; p = 0,000).

When the trust for the mobile operator/manufacturer to share location data with the government to study or mitigate the spread of COVID-19 increases, the trust for app developers to share it with the government also increases (rho = 0,543; p = 0,000). When the trust in the mobile operator/manufacturer using location data to study or mitigate the spread of COVID-19 rises, the trust in the app developers using location data rise (rho = 0,512; p = 0,000). When the COVID-19 test is positive, if the trust for the mobile operator/manufacturer sharing location data with the government decreases, the trust for the app developers sharing location data also decreases (rho = 0,642; p = 0,000). When the COVID-19 test is positive, if the trust for the mobile operator/manufacturer to share location data with everyone increases, the trust for the application

developers to share location data with everyone increases too (rho = 0,581; p = 0,000). The higher the confidence in a mobile operator/manufacturer sharing location data with the government to investigate or mitigate the spread of COVID-19, the higher the confidence in sharing location data with the government prior to COVID-19 (rho = 0,488; p = 0.000). For the trust for the application developers to share location data with the government to study or mitigate the spread of COVID-19 gets higher, the trust for the sharing location data with the government before the COVID-19 also gets higher (rho = 0,356; p = 0,000). And finally, there is a significant positive correlation between the trust in sharing data with the Health Ministry of Turkey and with Public Health Authorities (rho = 0,593; p = 0,000) and with hospitals (rho = 0,500; p = 0,000) and with Local Law Enforcement (rho = 0,543; p = 0,000).

According to the Mann-Whitney U test, there is a significant difference between people who allow and who do not allow access to location information in terms of the trust for sharing location data with mobile operators/manufacturers to study or mitigate the spread of COVID-19 (U = 13843; p = 0,000). There is a significant difference between people who allow and who do not allow access to location information in terms of the trust for the sharing of location data with app developers to study or mitigate the spread of COVID-19 (U = 14958; p = 0,000). Last, but not least, there is a significant difference between those who thought that GCMR would be useful for public health and those who thought that it would be useful in terms of willingness to share their data (U = 330; p = 0,000). The people, who thought that the report would be beneficial, expressed their willingness to share their data.

11.5. Discussion

When starting this study, our opinion was that the digital literacy rates of the participants were low. On the contrary, in the survey results, the digital literacy level was very high. We attribute this to the high education level of the respondents. When we looked at the questions measuring knowledge about technology, both male and female respondents knew how to change location permissions. It was understood that the majority of the participants did not read the terms and conditions statements. Interestingly, most applications used on phones have terms and conditions and individuals who say that they are sensitive to data privacy do not actually read the statements according to our survey results. With our study, we have proved that the digital literacy rate of the elderly is low. In the survey data, it was observed

that young participants were knowledgeable about privacy settings and location permissions, while this information was scarce for older participants. In addition, considering the level of education and technology competence, it is concluded that the participants with higher education levels are more competent.

The saying "If you're not paying for the product, you are the product" of Tim O'Reilly (Twitter 2.09.2010) has shown its true meaning in these times. Mobile applications require some permissions from users when downloaded. In the research of T. Sharma and M. Bashir (2020), it was determined that 30 out of 50 applications requested access to the users' data (location access permission, camera access permission, etc.) on mobile devices. In our study, when an imaginary application requested various permissions to examine or mitigate the spread of COVID-19, the majority of the participants did not want to give consent to these permissions. Contrarily, their tendency to allow access to location information was higher. This may be due to the fact that most of contact tracing applications require location information.

When we asked which personal data they think Google Maps can access out of e-mail, name, current location, home address, phone/device type, current workplace/employer and hobbies, the majority of the participants selected location data. As Mary Atamaniuk (2020) stated in her article, which analyzes the personal data use of the world's leading brands, Google can actually access all these data. Mary Atamaniuk attributed this to people clicking "accept" in a cookie popup window without reading any information. Our survey concluded that the majority of the participants did not read the service contracts, which supports M. Atamaniuk's opinion.

The vast majority of respondents said they were very concerned about COVID-19 and thought that social distancing was an important tool to prevent the spread of COVID-19. It was understood from the answers that a small number of participants who did not believe in social distancing frequently took public transportation. The majority of people with a high degree of concern said that they had little or no visits to places such as restaurants and parks. The vast majority of respondents with a high COVID-19 anxiety level stated that they were generally at their homes during the pandemic. They said that they rarely or never visited places such as restaurants, public transportation, workplaces, and parks. Even participants who think social distance is insignificant to preventing COVID-19 have spent the majority of their time in their homes. This may be due to the imposed lockdowns. Participants with low income stated that they used public

transportation more frequently. Unfortunately, even if we are faced with a lethal virus, individuals with low incomes, due to economic reasons, are in more risky environments.

Most participants did not know anything about the GCMR, which Google released using location data to measure community movements and slow the spread of COVID-19. It was a surprising result that the participants with a high degree of digital literacy did not know anything about the report. The minority of the respondents who knew the report said they thought the report was beneficial for stopping COVID-19.

In our study, when we asked the participants with different scenarios about how they would feel if mobile phone manufacturers/operators, app developers and the government use location data to examine or mitigate the spread of COVID-19, the majority said they would be uncomfortable with this scenario. Results showed that the opinions of the participants on this issue were more positive if their COVID-19 tests were positive. Participants who found the GCMR useful for slowing the spread of the COVID-19 said that they could share their personal location data for the benefit of public health. This shows that to fight the virus, respondents are willing to share their data voluntarily with the authorities ignoring their privacy.

Again, in this scenario, half of the participants were annoyed by the use of location data by mobile phone manufacturers/operators or application producers, and more disturbed by the sharing of their data with the government. The answers of the participants were consistent with their previous answers. For example, those who allow location information access also said that mobile phone manufacturers/operators or application manufacturers also allow the use of location data for the same purposes.

Half of the participants were disturbed by the view that the Turkish Ministry of Health or certain units of the government use location data for the same purposes, while the other half were undecided. We think this is due to the fact that most individuals are unsure of what to do, as the virus suddenly entered our lives and changed the world. Individuals had to choose between their health, digital privacy, and economic well-being. This increased their indecision. As Bekir Agırdır mentions, people rely on technology, but they do not trust the people managing technology in Turkey (Instagram [n.d.]).

As with L. Simko et al. (2020) research, more than half of the participants in our study are concerned about data sharing with the government. When we asked the same questions for before and after the COVID-19 scenarios, the

vast majority of the participants said that they would not want to share their location data with the government. They even thought that their personal data collected by the authorities during the pandemic would not be deleted in the future when everything was over. When we asked about the HES application developed by the Turkish Ministry of Health to reduce COVID-19, the participants said that most of them downloaded the application and the reason for downloading was to see the density of cases around them.

All these results showed that individuals are very concerned with their health and data privacy. But they are confused as to what to do to protect their privacy.

11.6. Implications for practice

If our survey could be conducted both online and traditionally offline, we could reach a wider audience in terms of demography. Therefore, this research can be repeated after the COVID-19 pandemic. This way we might be able to observe if there is a change in the opinions of the participants after the pandemic. In this manner, people who do not have digital literacy and the older (+65 of age) audience could be reached.

According to the survey responses, the majority of the participants thought that the data collected during the COVID-19 period would be used after the pandemic. Therefore, such a study can be repeated to observe whether this concern of the participants would change in the future.

Conclusion

Google Community Mobility Reports and similar reports are actually useful in terms of preventing COVID-19 and are open to all users. The result of our study shows that individuals need to know more about reports like GCMR. Such useful reports should become more common. It is very important to ensure that the personal data collected by the monopolized big technology companies and public authorities during the pandemic are used only to prevent COVID-19, so as not to prevent the rights and freedoms of individuals in the future. In order to prevent this, efforts should be made to use the data proportionately, in accordance with ethical rules and sensitive to privacy with state supervision by experts in the field. In addition,

in order to prevent future generations from being spied on by the digitized Big Brother, data usage must be limited, regulated by the law, and strict sanctions should be imposed for the misuse of data. These implementations should ensure a "consent mechanism" between the parties.

Governments and tech companies should consider ethical issues when implementing contact tracing technology in order not to face resistance from users. To do that, the "data-first" approach seems preferable. This is because our study observed that participants approved applications without reading the terms and conditions, despite having a high level of digital literacy. This shows that their awareness of the protection of their personal data is not strong enough.

According to the results of our study, the participants attach importance to privacy and worry about the spread of COVID-19. They are uncertain about what purposes their personal data will be used for in the future. Despite this, they do not hesitate to share their personal data for the benefit of public health. Perhaps the most important of the results we learned from this research is that the participants are very concerned about their personal data after the pandemic is over. These results should be taken into account by non-governmental organizations, authorities and large technology companies without causing eroded privacy and widespread adoption of new surveillance tools. User data and different algorithms should be handled in a responsible manner and be privacy-sensitive, then we can achieve a democratic and open world without sacrificing public trust.

References

Abeler, J., M. Bäcker, U. Buermeyer, H. Zillessen (2020), *COVID-19 Contact Tracing and Data Protection Can Go Together*, "JMIR mHealth and uHealth" 8(4): 1–5. DOI: https://doi.org/10.2196/19359.

Ahn, N.Y., J.E. Park, D.H. Lee, P.C. Hong (2020), *Balancing Personal Privacy and Public Safety During COVID-19: The Case of South Korea*, "IEEE Access" 8: 171325–171333. DOI: https://doi.org/10.1109/ACCESS.2020.3025971.

Aktay, A., S. Bavadekar, G. Cossoul, J. Davis, D.D. Desfontaines, R.J. Wilson (2020), *Google COVID-19 Community Mobility Reports: Anonymization Process Description (Version 1.0)*, 1–5, arXiv preprint arXiv:2004.04145, https://arxiv.org/abs/2004.04145 (12.12.2020).

Anderson, R.M., H. Heesterbeek, D. Klinkenberg, T.D. Hollingsworth (2020), *How Will Country-Based Mitigation Measures Influence the Course of the COVID-19 Epidemic?*, "The Lancet" 395(10228): 931–934. DOI: https://doi.org/10.1016/S0140-6736(20)30567-5.

Atamaniuk, M. (2020), *Which Company Uses the Most of Your Data?*, https://clario.co/blog/which-company-uses-most-data/ (18.12.2020).

Azad, M.A., J. Arshad, S.M. Akmal, F. Riaz, S. Abdullah, M. Imran, F. Ahmad (2020), *A First Look at Privacy Analysis of COVID-19*, "IEEE Internet of Things Journal" 8(21): 15796–15806. DOI: https://doi.org/10.1109/JIOT.2020.3024180.

Barrios, J.M., E. Benmelech, Y.V. Hochberg, P. Sapienza, L. Zingales (2021), *Civic Capital and Social Distancing During the COVID-19 Pandemic*, "Journal of Public Economics" 193: 104310. DOI: https://doi.org/10.1016/j.jpubeco.2020.104310.

Barro, R.J., J.F. Ursúa, J. Weng (2020), *The Coronavirus and the Great Influenza Pandemic: Lessons from the "Spanish Flu" for the Coronavirus's Potential Effects on Mortality and Economic Activity (No. w26866)*, "National Bureau of Economic Research," https://www.nber.org/papers/w26866 (5.12.2020).

Basellini, U., D. Alburez-Gutierrez, E.D. Fava, D. Perrotta, M. Bonetti, C.G. Camarda, E. Zagheni (2020), *Linking Excess Mortality to Google Mobility Data During the COVID-19 Pandemic in England and Wales*, 1–18, SocArXiv. DOI: https://doi.org/10.31235/osf.io/75d6m.

BBC News Turkey (16.01.2021), *WhatsApp Postponed the Change of Privacy Agreement Regarding Data Sharing*, https://www.bbc.com/turkce/haberler-dunya-55684775 (19.02.2021).

Beaunoyer, E., S. Dupéré, M.J. Guitton (2020), *COVID-19 and Digital Inequalities: Reciprocal Impacts and Mitigation Strategies*, "Computers in Human Behavior" 111: 106424. DOI: https://doi.org/10.1016/j.chb.2020.106424.

Bengio, Y., D. Ippolito, R. Janda, M. Jarvie, B. Prud'homme, J.-F. Rousseau, Y.W. Yu (2020), *Inherent Privacy Limitations of Decentralized Contact Tracing Apps*, "Journal of the American Medical Informatics Association" 28(1): 193–195. DOI: https://doi.org/10.1093/jamia/ocaa153.

Berke, A., M. Bakker, P. Vepakomma, K. Larson, A. Pentland (2020), *Assessing Disease Exposure Risk with Location Data: A Proposal for Cryptographic Preservation of Privacy*, 1–15, arXiv preprint 2003.14412, https://arxiv.org/abs/2003.14412 (2.12.2020).

Borger, J. (7.01.2021), *Maga Mob's Capitol Invasion Makes Trump's Assault on Democracy Literal*, https://www.theguardian.com/us-news/2021/jan/06/us-capitol-trump-mob-election-democracy (21.01.2021).

Brough, A.R., K.D. Martin (2020), *Consumer Privacy During (and after) the COVID-19 Pandemic*, "Journal of Public Policy & Marketing" 40(1): 108–110. DOI: https://doi.org/10.1177/0743915620929999.

BTK, Information and Communication Technologies Authority (2020), Communications Services Statistics (Communication Services Statistics), Istanbul, Turkey, https://www.btk.gov.tr/uploads/pages/iletisim-hizmetleri-istatistikleri/istatistik-2020-3.pdf (1.01.2021).

Buchholz, B.A., J. DeHart, G. Moorman (2020), *Digital Citizenship During a Global Pandemic: Moving Beyond Digital Literacy*, "Journal of Adolescent & Adult Literacy" 64(1): 11–17. DOI: https://doi.org/10.1002/jaal.1076.

Carli, A. De, M. Franco, A. Gassmann, C. Killer, B. Rodrigues, E. Scheid, D. Schoenbaechler, B. Stiller (2020), *WeTrace A Privacy-preserving Mobile COVID-19 Tracing Approach and Application*, 1–15, arXiv preprint, https://arxiv.org/abs/2004.08812v1 (3.01.2021).

Cho, H., D. Ippolito, Y.W. Yu (2020), *Contact Tracing Mobile Apps for COVID-19: Privacy Considerations and Related Trade-offs.*, 1–12, arXiv:2003.11511 [Cs], http://arxiv.org/abs/2003.11511 (13.01.2021).

Chunara, R., S.H. Cook (2020), *Using Digital Data to Protect and Promote the Most Vulnerable in the Fight Against COVID-19*, "Frontiers in Public Health" 8: 1–3. DOI: https://doi.org/10.3389/fpubh.2020.00296.

Coibion, O., Y. Gorodnichenko, M. Weber (2020), *The Cost of the COVID-19 Crisis: Lockdowns, Macroeconomic Expectations, and Consumer Spending (No. w27141)*, "National Bureau of Economic Research," https://www.nber.org/papers/w27141 (14.12.2020).

COVID-19 – Google Mobility Report (2020), https://datastudio.google.com/u/0/reporting/a529e043-e2b9-4e6f-86c6-ec99a5d7b9a4/page/yY2MB?s=ho2bve-3abdM (26.12.2020).

Díaz, A. (7.04.2020), *Coronavirus, Location Tracking, and Civil Liberties*, https://www.brennancenter.org/our-work/analysis-opinion/coronavirus-location-tracking-and-civil-liberties (18.12.2020).

Dogan, S. (2020), *From Google, COVID-19 Community Mobility Reports: Turkey*, https://medium.com/t%C3%BCrkiye/googledan-Covid-19-topluluk-hareketlili%C4%9Fi-raporu-t%C3%BCrkiye-3e052bb2cf87 (18.12.2020).

Dubov, A., S. Shoptaw (2020), *The Value and Ethics of Using Technology to Contain the COVID-19 Epidemic*, "The American Journal of Bioethics" 20(7): W7–W11. DOI: https://doi.org/10.1080/15265161.2020.1764136.

Fahey, R.A., A. Hino (2020), *COVID-19, Digital Privacy, and the Social Limits on Data--Focused Public Health Responses*, "International Journal of Information Management" 55: 1–5. DOI: https://doi.org/10.1016/j.ijinfomgt.2020.102181.

Fairchild, A.L., R. Bayer, J. Colgrove (2007), *Privacy and Public Health Surveillance: the Enduring Tension*, "Virtual Monitor" 9(12): 838–841. DOI: https://doi.org/10.1001/virtualmentor.2007.9.12.mhst1-0712.

Ferguson, N., D. Laydon, G. Nedjati Gilani, N. Imai, K. Ainslie, M. Baguelin, A. Ghani (2020), *Report 9: Impact of Non-Pharmaceutical Interventions (NPIs) to Reduce COVID19 Mortality and Healthcare Demand*, "Imperial College London": 1–20. DOI: https://doi.org/10.25561/77482.

Gilbert, G.L., C. Degeling, J. Johnson (2019), *Communicable Disease Surveillance Ethics in the Age of Big Data and New Technology*, "Asian Bioethics Review" 11(2): 173–187. DOI: https://doi.org/10.1007/s41649-019-00087-1.

Google (2020), *Google COVID-19 Community Mobility Reports*, https://www.google.com/covid19/mobility/ (7.11.2020).

Gvili, Y. (2020), *Security Analysis of the COVID-19 Contact Tracing Specifications by Apple Inc. and Google Inc.*, IACR Cryptol. ePrint Arch, 428, https://eprint.iacr.org/2020/428.pdf (22.12.2020).

Hayat Eve Sığar [n.d.], https://hayatevesigar.saglik.gov.tr/index-eng.html (12.12.2020).

Harari, Y.N. (20.03.2020), *The World after Coronavirus. The Financial Times*, https://www.ft.com/content/19d90 308-6858-11ea-a3c9-1fe6f edcca75 (12.11.2020).

Herren, C.M., T.K. Brownwright, E.Y. Liu, N. El Amiri, M.S. Majumder (2020), *Democracy and Mobility: A Preliminary Analysis of Global Adherence to Non-Pharmaceutical Interventions for COVID-19*, https://ssrn.com/abstract=3570206 (28.12.2020).

Huang, X., Z. Li, Y. Jiang, X. Ye, C. Deng, J. Zhang, X. Li (2020), *The Characteristics of Multi-source Mobility Datasets and How They Reveal the Luxury Nature of Social Distancing in the US During the COVID-19 Pandemic*, "medRxiv": 1–32. DOI: https://doi.org/10.1101/2020.07.31.20143016.

Hussein, M.R., A.B. Shams, E.H. Apu, M.S. Rahman, K.A. Mamun (2020), *Digital Surveillance Systems for Tracing COVID-19: Privacy and Security Challenges with Recommendations*, 1–6, arXiv preprint arXiv:2007.13182., https://arxiv.org/abs/2007.13182v1 (2.12.2020).

Huynh, T.L. (2020), *Does Culture Matter Social Distancing Under the COVID-19 Pandemic?*, "Safety Science" 130:1–7. DOI: https://doi.org/10.1016/j.ssci.2020.104872.

Ienca, M., E. Vayena (2020), *On the Responsible Use of Digital Data to Tackle the COVID-19 Pandemic*, "Nature Medicine" 26(4): 463–464. DOI: https://doi.org/10.1038/s41591-020-0832-5.

Intersoft Consulting (2016), General Data Protection Regulation GDPR, https://gdpr-info.eu/ (11.05.2023).

Instagram, Bekir Agırdır [27.01.2021], https://www.instagram.com/reel/CKjaH-Chl6Mj/?igshid=1ss59ktae5awh (19.02.2021).

Jung, G., H. Lee, A. Kim, U. Lee (2020), *Too Much Information: Assessing Privacy Risks of Contact Trace Data Disclosure on People with COVID-19 in South Korea*, "Frontiers in Public Health" 8. DOI: https://doi.org/10.3389/fpubh.2020.00305.

Klein, N. (13.05.2020), *How Big Tech Plans to Profit from the Pandemic*, https://www.theguardian.com/news/2020/may/13/naomi-klein-how-big-tech-plans-to-profit-fromcoronavirus-pandemic (6.01.2021).

Laing, T. (2020), *The Economic Impact of the Coronavirus 2019 (COVID-2019): Implications for the Mining Industry*, "The Extractive Industries and Society" 7(2): 580–582. DOI: https://doi.org/10.1016/j.exis.2020.04.003.

Lee, L.M., Ch.M. Heilig, A. White (2012), *Ethical Justification for Conducting Public Health Surveillance Without Patient Consent*, "American Journal of Public Health" 102(1): 38–44. DOI: https://doi.org/10.2105/AJPH.2011.300297.

Leins, K., C. Culnane, B.I. Rubinstein (2020), *Tracking, Tracing, Trust: Contemplating Mitigating the Impact of COVID-19 Through Technological Interventions*, "The Medical Journal of Australia" 213(1): 6–8.e1. DOI: https://doi.org/10.5694/mja2.50669.

Martin, K.D., A. Borah, R.W. Palmatier (2017), *Data Privacy: Effects on Customer and Firm Performance*, "Journal of Marketing" 81(1): 36–58. DOI: https://doi.org/10.1509/jm.15.0497.

Mathews, L. (13.04.2020), *500,000 Hacked Zoom Accounts Given Away for Free on The Dark Web*, https://www.forbes.com/sites/leemathews/2020/04/13/500000-hacked-zoom-accounts-given-away-for-free-on-the-dark-web/?sh=7542574b58c5 (20.01.2021).

Michael, K., R. Abbas (2020), *Behind COVID-19 Contact Trace Apps: The Google–Apple Partnership*, "IEEE Consumer Electronics Magazine" 9(5): 71–76. DOI: https://doi.org/10.1109/MCE.2020.3002492.

Nature (4.02.2021), *COVID Research Updates: What Makes a Person with COVID More Contagious? Hint: Not a Cough*, https://doi.org/10.1038/d41586-020-00502-w (5.02.2021).

Oliver, N., B. Lepri, H. Sterly, R. Lambiotte, S. Deletaille, M. De Nadai, P. Vinck (2020), *Mobile Phone Data for Informing Public Health Actions Across the COVID-19 Pandemic Life Cycle*, "Sci Adv" 6(23): 1–6. DOI: https://doi.org/10.1126/sciadv.abc0764.

Phillips, T., H. Ellis-Petersen, S. Walker, J.C. Wong (17.01.2021), *Trump Social Media Ban Sparks Calls for Action Against other Populist Leaders*, https://www.theguardian.com/media/2021/jan/17/trump-social-media-ban-jair-bolsonaro-narendra-modi (21.01.2021).

Raskar, R., I. Schunemann, R. Barbar, K. Vilcans, J. Gray, P. Vepakomma, J. Werner (2020), *Apps Gone Rogue: Maintaining Personal Privacy in an Epidemic*, 1–15, arXiv preprint arXiv:2003.08567, https://arxiv.org/abs/2003.08567 (5.12.2020).

Roberts, M. (3.02.2021), *UK Finds More Coronavirus Cases with 'Concerning' Mutations*, https://www.bbc.com/news/health-55900625 (5.02.2021).

Romm, T., D. Harwell, E. Dwoskin, C. Timberg (10.04.2020), *Apple, Google Debut Major Effort to Help People Track if They've Come in Contact with Coronavirus*,

https://www.washingtonpost.com/technology/2020/04/10/apple-google--tracking-coronavirus/(17.01.2021).

Saha, J., B. Barman, P. Chouhan (2020), *Lockdown for COVID-19 and Its Impact on Pupil Mobility in India: an Analysis of the COVID-19 Community Mobility Reports*, "Children and Youth Services Review" 116: 1–14. DOI: https://doi.org/10.1016/j.childyouth.2020.105160.

Sharma, T., M. Bashir (2020), *Use of Apps in the COVID-19 Response and the Loss of Privacy Protection*, "Nature Medicine" 26: 1165–1167. DOI: https://doi.org/10.1038/s41591-020-0928-y.

Silva, G.C. da, S. Oliveira, E.F. Wanner, L.C.T. Bezerra (2020), *Google COVID-19 Community Mobility Reports: Insights from Multi-criteria Decision Making*, 1–11, arXiv e-prints, arXiv-2009, https://arxiv.org/abs/2009.10648 (5.11.2020).

Simko, L., R. Calo, F. Roesner, T. Kohno (2020), *COVID-19 Contact Tracing and Privacy: Studying Opinion and Preferences*, 1–32, arXiv preprint arXiv:2005.06056v1, https://arxiv.org/abs/2005.06056 (5.12.2020).

Singer, N., C. Sang-Hun (24.03.2020), *As Coronavirus Surveillance Escalates, Personal Privacy Plummets*, https://www.nytimes.com/2020/03/23/technology/coronavirus- surveillance-tracking-privacy.html (13.01.2020).

Stanley, J., J.S. Granick (2020), *The Limits of Location Tracking in an Epidemic*, "American Civil Liberties Union": 1–9, https://www.aclu.org/sites/default/files/field_document/limits_of_location_tracking_in_an_epidemic.pdf (22.11.2020).

Sun, R., W. Wang, M. Xue, G. Tyson, S. Camtepe, D. Ranasinghe (2020), *Vetting Security and Privacy of Global COVID-19 Contact Tracing Applications*, 1–13, arXiv preprint arXiv:2006.10933, https://arxiv.org/abs/2006.10933 (12.12.2020).

T.C. Sağlık Bakanlığı (2.05.2020), *COVID-19 (SARS-CoV-2) Infection Guide*, https://covid19bilgi.saglik.gov.tr/depo/rehberler/Covid-19_Rehberi.pdf (26.11.2020).

Twitter, Tim O'Reilly (2.09.2010), https://twitter.com/timoreilly/status/22823381903 (18.12.2020).

Vitak, J., M. Zimmer (2020), *More Than Just Privacy: Using Contextual Integrity to Evaluate the Long-Term Risks from COVID-19 Surveillance Technologies*, "Social Media + Society": 1–4. DOI: https://doi.org/10.1177/2056305120948250.

Wang, H., N. Yamamoto (2020), *Using a Partial Differential Equation with Google Mobility Data to Predict COVID-19 in Arizona*, "Mathematical Biosciences and Engineering" 17(5): 4892–4904. DOI: https://doi.org/10.3934/mbe.2020266.

Wen, H., Q. Zhao, Z. Lin, D. Xuan, N. Shroff (2020), *A Study of the Privacy of COVID-19 Contact Tracing Apps*, [in:] N. Park, K. Sun, S. Foresti, K. Butler, N. Saxena (eds.), *Security and Privacy in Communication Networks. 16th EAI International Conference, SecureComm 2020, Washington, DC, USA, October 21–23, 2020, Proceedings,* Part I (Cham: Springer): 297–317. DOI: https://doi.org/10.1007/978-3-030-63086-7_17.

Whaiduzzaman, M., M.R. Hossain, A.R. Shovon, S. Roy, A. Laszka, R. Buyya, A. Barros (2020), *A Privacy-preserving Mobile and Fog Computing Framework to Trace and Prevent COVID-19 Community Transmission*, "IEEE Journal of Biomedical and Health Informatics" 24(12): 3564–3575. DOI: https://doi.org/10.1109/JBHI.2020.3026060.

Whittaker, Z. (20.04.2020), *Hundreds of Academics Back Privacy-Friendly Coronavirus Contact Tracing Apps*, https://techcrunch.com/2020/04/20/academics-contact-tracing/ (17.01.2021).

WHO (2020), *WHO Director-Generals Opening Remarks at the Media Briefing on COVID-19*, World Health Organization, https://www.who.int/director-general/speeches/detail/who-director-general-s-opening-remarks-at-the-media-briefing-on-Covid-19---11-march-2020 (17.01.2021).

WHO (16.02.2021), *Weekly Epidemiological Update*, World Health Organization, https://www.who.int/publications/m/item/weekly-epidemiological-update---16-february-2021 (19.02.2021).

Wielechowski, M., K. Czech, Ł. Grzęda (2020), *Decline in Mobility: Public Transport in Poland in the Time of the COVID-19 Pandemic*, "Economies" 8(4): 78. DOI: https://doi.org/10.3390/economies8040078.

Yilmazkuday, H. (2021), *Stay-at-home Works to Fight Against COVID-19: International Evidence from Google Mobility Data*, "Journal of Human Behavior in the Social Environment" 31(1–4): 210–220. DOI: https://doi.org/10.1080/10911359.2020.1845903.