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

Elsevier hereby grants permission to make all its COVID-19-related research that is available on the COVID-19 resource centre - including this research content - immediately available in PubMed Central and other publicly funded repositories, such as the WHO COVID database with rights for unrestricted research re-use and analyses in any form or by any means with acknowledgement of the original source. These permissions are granted for free by Elsevier for as long as the COVID-19 resource centre remains active.
Complex Adaptive Systems Conference Theme: Big Data, IoT, and AI for a Smarter Future
Malvern, Pennsylvania, June 16-18, 2021

Digital Surveillance Technologies to Combat COVID-19: A Contemporary View
Mohamad Kassab\textsuperscript{a}, Valdemar Vicente Graciano Neto\textsuperscript{b}

\textsuperscript{a}Pennsylvania State University, Malvern, P.A. USA
\textsuperscript{b}Universidade Federal de Goiás (UFG), Goiânia, GO, Brazil

Abstract
Since the genesis case was confirmed in Wuhan, China in late 2019, the Novel Coronavirus Disease 2019 (COVID-19) has been spreading all over the world at an accelerating rate. Almost immediately, IoT technologies were deployed in various surveillance scenarios as part of an effort to combat the pandemic. Among the emerging solutions, contact tracing mobile applications have been playing an effective role to help stem the spread of the virus by tracking individuals and those they come into exposure with. This paper aims at providing a panoramic view of the digital tracking technologies that have been utilized so far in response to the pandemic. We particularly provide a detailed analysis of 47 contact tracing mobile applications that emerged in response to COVID-19. We accompany our analysis with a discussion on the privacy and the technology / social constraints that may challenge the deployment of these applications as digital surveillance platforms.

© 2021 The Authors. Published by Elsevier B.V.
This is an open access article under the CC BY-NC-ND license (https://creativecommons.org/licenses/by-nc-nd/4.0)
Peer-review under responsibility of the scientific committee of the Complex Adaptive Systems Conference, June 2021.

Keywords: COVID; Digital Surveillance; Contact Tracing; Privacy.

1. Introduction
The novel coronavirus (SARS-COV-2) that causes the Coronavirus Disease 2019 (COVID-19) has been spreading worldwide at an accelerated rate. The situation was declared a pandemic by the World Health Organization (WHO) on March 11, 2020. By mid of July 2020, the number of reported COVID-19 cases surpassed 13 million worldwide with a 4.5% mortality rate according to the data from John Hopkins University & Medicine
Corona Virus Resource Center\footnote{https://coronavirus.jhu.edu/map.html}. Almost immediately, governments around the world started to pursue containment measures to help slow the spread of the virus.

Digital surveillance has been deployed as part of these measures to i) track confirmed and potentially impacted cases with the virus, ii) enforce lockdown when necessary, and iii) generate a much-needed source of data and statistics to the authorities.

The Internet of Things (IoT) community has been stimulated with the COVID-19 outbreak to conceive solutions to combat the pandemic. IoT protocols (e.g., Bluetooth Low Energy (BLE), Near-Field Communications (NFC), RFID, GPS, and WiFi) are receiving great attention for providing solutions spanning the spectrum from a biosensor capable of detecting the SARS-COV-2 virus in the air \cite{1} to the rapidly emerging digital surveillance technologies to track individuals and crowds. A digital surveillance for an individual relies on the unique identifiers that are either temporally (RFID tags) or permanently assigned to a person like personal identifiers, and a way to sample individual’s locations, either on short or long temporal scales for authorities to keep track of the citizens or temporary residents.

As of July 2020, approximately 5400 articles, including peer-reviewed and newspaper articles, were found in the PennState LionSearch tool as a result of the search query “(Digital tracking) and (COVID)”. LionSearch is an integrated search engine of books, e-books, research articles, newspaper articles, and other publications integrated from over 950 database/search engines, including over 80 databases/search engines for healthcare/medicine discipline and over 15 for computer/software/information science and engineering. The tool is provided and maintained by the Pennsylvania State University’s Library. The textual analysis of these publications highlights that two broad classes of technologies have been utilized to establish digital tracking (i) Non-mobile technologies (e.g., tracking bracelets, cameras with thermal sensors, drones, etc.), and (ii) mobile technologies (e.g., smartphones with inbuilt location sensors, contact tracing mobile-based applications).

Despite the avalanche of emerging surveillance technologies to combat the pandemic, there is still little knowledge of how these could affect society. For example, how widely the contact tracing mobile applications are being used? What type of data will they collect, and how data will be saved? Whom is it shared with? And are there policies in place to prevent abuse?

This paper aims at providing a panoramic view of the digital tracking technologies that have been utilized so far in response to the pandemic. We will particularly present a detailed analysis of 47 contact tracing mobile applications that have recently emerged in response to COVID-19. We accompany our analysis with a discussion on the privacy and the social/technical constraints that may challenge the deployment of these applications as digital tracking platforms.

The remaining of the paper is structured as follows: Section 2 provides an overview of Digital tracking with non-mobile technologies, while Section 3 provides an overview of Digital tracking with mobile technologies. Section 4 discusses the privacy concerns with contact tracing applications while section 5 provides a discussion on the technology and social constraints. Section 6 concludes the paper.

2. Digital tracking with non-mobile technologies

At the most general level, surveillance of humans can be defined as “regard or attendance to others (whether a person, a group or an aggregate as with a national census) or to factors presumed to be associated with these. A central feature is gathering some form of data connectable to individuals (whether as uniquely identified or as a member of a category)” \cite{2}. Governments have been increasingly adopting extensive physical surveillance measures in response to the COVID-19 spread. Our review identified 64 digital tracking measures deployed in 38 countries (See: https://bit.ly/2Zpmhgy). We mapped these measures into two broad classes: Mobile and non-mobile based technologies.

The sphere of IoT non-mobile technologies during the pandemic includes variations from the usage of electronic bracelets, deployment of cameras equipped with thermal sensors and facial recognition software, surveillance drones...
used to monitor mass gatherings, to extensive CCTV networks in a bid to help enforce curfews. Our review identified 15 of the non-mobile based measures that were taken in 12 countries (See: https://bit.ly/2Zpmhgy). For example, in Hong Kong, all people traveling from China, Taiwan, and Macau received a bracelet to track their movements. In West Virginia, a judge has approved strapping ankle monitors to positively tested citizens who refuse to quarantine [3].

In Bahrain, electronic wristbands that are compatible with the country’s coronavirus contact tracing application “BeAware” has been in use to ensure infected citizens remain quarantined. Individuals wearing the electronic bracelet must be connected to the application at all times via Bluetooth and with GPS enabled to track movement [4].

Corporate IoT proximity detection and contact tracing devices have also been developed. An example comprises the LoRaWAN devices [5], which detect proximity and contact tracing among employees in areas like offices and trigger alarms to alert people they should keep a safe distance. Surveillance accompanied with facial recognition cameras equipped with enabled body temperature detection sensors has spread rapidly in China as the Chinese government is promoting the development of artificial intelligence (AI) that prioritizes the prevention of COVID-19 spread. The number of facial recognition cameras in use in China has indeed jumped 3.5 times in the past three years to reach 626 million deployed cameras in 2020 [6]. This motivated the government to take regulating measures to ensure the privacy of the collected biometric data through the “Personal Information Security Specifications”. This regulation states that collection, processing, transfer, and disclosure of Personal Information data should be for justified, legal necessity, and often to require consent, and must be kept secure. But the principles of this regulation are not reflective of the current reality of the Chinese facial recognition ecosystem, where sensitive biometric data is frequently collected without consent or sufficient data privacy protections, particularly amid the COVID-19 outbreak.

Hoping to spot symptoms of the virus among the public, the authority in Dubai are also utilizing security cameras fitted with facial recognition software and thermal imaging technology. Similar thermal imaging surveillance cameras have also been tested in Bournemouth Airport, United Kingdom.

The resort city of Cannes on the Cote d’Azur has trialed innovative cameras in outdoor markets and on buses, equipped with AI software that generates an automatic alert to city authorities on where breaches of the mask and distancing rules are spotted. The French firm “Datakalab” [7] insists that its technology sets apart from the kind of hi-tech surveillance common in China as their system doesn’t store any identifying data, but only sends anonymized alerts to the authorities.

Surveillance drones equipped with sensors and cameras have been also used to enforce lockdown. For example, the New York Police Department has been using aerial photography to monitor lockdown measures.

3. Digital tracking with mobile technologies

The smartphone-enabling technologies such as Bluetooth, RFID tracking, built-in sensors, and NFC allow it to be an integral part of the IoT sphere and to be the most used devices in these environments. For the digital tracking purpose during the COVID-19 crisis, authorities have strongly relied on mobile technologies. We identified 50 mobile-related digital tracking measures utilized in 34 countries. These can be further mapped into two classes discussed below.

3.1 Authorities accessing individual or aggregated data directly from mobile operators

At least in 11 countries, mobile operators were reported to share individualized location data with authorities to ensure lockdown compliance. For example, in New Zealand, residents arriving from overseas were texted by the Police asking if they consent to be monitored via their cell phone [8].

Mobile operators have been also sharing aggregated data with the authorities to facilitate the analysis of how citizens have reacted to regulations on social distancing. For instance, Vodafone in Italy reported on its website that it will be willing to assist governments in developing insights based on large anonymized data sets by generating an aggregated heat map for the Lombardy region to “help the authorities to better understand population movements to help thwart the spread of COVID-19” [9]. A similar heatmap has been generated in Argentina as well [19].
3.2 Mobile Applications

There has been a flood of mobile applications in the middle of the battle with COVID-19. For example, in Poland, an application for quarantined patients asks to randomly take geo-located selfies. A similar application was deployed in Russia where citizens with suspected COVID-19 in Moscow asked to send selfies 3 times a day to authorities. In Turkey, the Quarantine enforcement application, ‘Life Fits Inside the House’, was deployed to monitor citizens [10].

Wuhan, China, where the first cases of novel coronavirus were reported, opened its border with a condition imposing the installation of a government surveillance mobile application as a requirement for the entry/exit for the region. The government then tracks its citizens through the installed software by analyzing their data to sort individuals into color-coded categories - red, yellow, or green - corresponding to their health status and level of risk for COVID-19.

On the other hand, starting the month of April 2020, we saw an uptick in the number of a particular category of mobile applications to help stem the spread of the virus by tracking individuals and those they come into exposure with; namely “proximity contact tracing applications”. As of July 2020, there were at least 47 contact tracing applications available for 29 countries (Please see the list of the applications provided through the link: https://bit.ly/3fMGWRm). This includes the recently announced Google/Apple opt-in contact- tracing application using phones Bluetooth connection to deliver exposure notifications for Android or iOS users (see the described scenario at Google blog: https://bit.ly/3cwZvYt).

Figure 1 provides the world-wide distribution for the analyzed contact tracing applications in response to the COVID-19 pandemic along with the approximate volume of downloads as of July 2020.

While these tracing applications may have slightly different approaches on how tracing contacts, at their core, they are tracking programs using Bluetooth or GPS to track an individual’s exposure to cases. Users elect to share data and are alerted if they have been within proximity to COVID-19 cases. If an individual is found to be infected with the virus, all of the people that have recently been near him/her are alerted and asked to follow the public health authorities’ guidelines. Not all existing contact-tracing applications serve as digital tracking applications from the authority perspective. Depending on the application design, Public Health Authorities may (or not) receive data that users choose (or asked) to share to enhance contact tracing. Figure 2 provides an aggregated contemporary view of the analyzed applications.

Fig. 1. Distribution of COVID-19 Contact Tracing Mobile Applications as of July ‘20 along with the approximate volume of downloads.
We further analyzed the applications against the mechanisms they employ for data collection and management. Only 15% of these applications were detected collecting anonymous data with no Personally Identifiable Information (PII). 43% of the applications maintain Pseudonymized copies of the data, while the remaining 42% of the applications had no information on the data anonymity. We report the list of the PII collected per application through the link: https://bit.ly/3fMGWRm. Once collected, 47% of the applications then stored the data in a centralized location (e.g. authority server), while 26% retained the data locally on the mobile device. 28% of the applications didn’t report on how the data will be stored. The majority of these applications (58%) don’t provide sufficient information regarding the data storage duration though. Only 21% of these applications reported temporary storage, while the remaining 21% store collected data for a period of one year or longer. Forty-Seven Percent of these applications will store data in unencrypted format comparing to only 21% that store encrypted data. Blockchain-based contact-tracing applications constitute (23%) of these applications. With the “decentralization” and “immutability” blockchain characteristics, many of the designed contact tracing applications are utilizing a single shared ledger to store some of the identity metadata (whenever they are created), while mitigating the traditional threats to privacy due to the centralization aspects of a traditional database or cloud environment. For example, a recently constructed open-source application in India using Ethereum Blockchain allows citizens to voluntarily participate in a program that anonymously records their location history [11]. If there are any infected people with a travel or location history originating from a particular place, the other users who were present in the close vicinity will be warned of the incident, to put them on close observation as a precaution. Storing all of the information on Ethereum is done with zero-knowledge proofs so that the identity of individuals remains pseudonymous. Another blockchain-based contact tracing application is DP3T being developed in Europe [12].

While the avalanche of the digital proximity tracking technologies for COVID-19 contact tracing is understandable at the time of the pandemic, there must be ethical considerations to guide their use. The Centers for Disease Control and Prevention (CDC) defined the preliminary criteria for minimum and preferred characteristics of digital contact tracing tools to help health departments overcome the challenges in the COVID-19 contact tracing workflow (See: https://bit.ly/3fLAMSh). The World Health Organization also published interim guidance in May
2020 to regulate these applications [13]. Next, we will elaborate further on the privacy and technology/social constraints challenges that accompany the deployment of contact tracing mobile applications as tracking instruments.

4. Privacy Concerns with Contact Tracing Applications

While several countries are racing to develop digital tools to improve the proximity contact tracing to control the COVID-19 virus spread, the mad dash has left some places with a confusing mishmash of options and the software security researchers’ community has worried about vulnerabilities in hastily written software. For example, only 25% of the existing proximity tracing applications provide privacy policies, while only (58%) don’t disclose how long they will store users’ data for and about (60%) have no publicly stated anonymity measures.

Besides, code relating to Google advertising and tracking platforms (e.g., Google AdSense, DoubleClick) has been detected in at least 14 contact tracing applications. We also found code relating to Facebook advertising and tracking in 8 of these analyzed applications. Such a code allows publishers to make money by showing advertisements to their users from a vast array of sources. The presence of such a tracking code in contact tracing applications raises privacy concerns due to the targeting options offered by Google / Facebook advertisements platforms.

Some of these applications are also blockchain-based [14]. Because of the blockchain’s “immutability” characteristic, users’ records can’t be changed or removed from the network. Will this be appropriate when a lockdown is lifted? The “finality” characteristic of the blockchain can also diverge from existing legislation such as the European GDPR or the recently announced Brazilian LGPD that provides all citizens the capacity to govern their data including the right to request an institution to delete personal data being processed based upon consent. In [12], the report stated that some privacy protection measurements by decentralized DP3T contact tracing app used in Europe might have the opposite effect of what they were intended to. Specifically, patients who were tested positive and that were reported might be deanonymized and private encounters may be disclosed.

 Recommending these applications is perhaps understandable in the heat of the early stages of the pandemic. However, much deliberation must be given towards considering the long-term consequences of building such digital infrastructure across society. A report published by a global public policy firm for the tech sector recalled that 49% of the world remains digitally unconnected and affirms that “virus fightback must start with the adoption of policies that enable countries to take advantage of great leaps in a pandemic-busting ingenuity” [15], [16]. The report remarks that while European countries are trying to position themselves in privacy-protecting approaches by complying with the GDPR, some Asian governments, like China and South Korea, have taken broad and aggressive approaches that rely on gathering, analyzing, and sharing vast amounts of personal data. The report also still highlights that across North and South America, there have been fewer and less-organized efforts by governments to develop contact tracing solutions than in other regions [15].

Although challenges to preserve security and privacy remain, recent studies have shown that users have felt more comfortable to use contact-tracing applications as the pandemic proceeds. For example, a survey was conducted by Metova firm, a leading provider of custom software solutions for IoT, with 2000 residents of the United States on contact tracing and exposure notification applications use in the fight against COVID-19. The survey found 77% of participants would want to be notified via their mobile phone if someone they recently came in contact with was tested positive for COVID-19, and 85% are willing to anonymously share a positive COVID-19 status for the greater good [17].

5. Technology and Social Constraints

Despite the reports indicating the high level of willingness among the general population to download contact tracing applications, and share data through [17], the actual numbers of downloads are still relatively slim. A recent study by the University of Oxford’s Big Data Institute estimates that at least 60% of the population in a given area would need to use automated contact tracing applications for it to be considered effective in containing the virus [18]. On March 20, 2020, Singapore became one of the first countries to deploy a voluntary contact-tracing app, “Trace-Together” (https://www.tracetogether.gov.sg/) but only about 26% of the population installed it two months after its inauguration. While some level of compliance is still better than none, the low rates of adoption in parts of the world is a challenge for these applications to provide any breakthrough. Besides, the lack of access to
smartphones can be an obstacle to these which rely on a high level of inclusion. A median of 76% of the population across 18 advanced economies surveyed has smartphones, compared with a median of only 45% of the population in emerging economies [19]. The dominant contact tracing application in a nation would have to be authorized and sponsored by a government health authority. This is practically the only effective way to ensure a large scale adoption of an application within a country. But such a sponsorship process may require precious weeks for different countries’ applications to be fully tested and integrated.

Also, all the existing contact tracing mobile applications rely on GPS and/or Bluetooth capabilities which are not highly reliable still. Bluetooth’s range, for example, is considerably wider than 6 feet which can trigger a high percentage of false positives regarding the exposure to the virus. Continuously enabled GPS/Bluetooth capabilities can also drain the battery quickly. A 2016 study found that with good signal strength, a battery of a GPS-enabled mobile phone depletes by 13% while a weak signal could cause the battery to drop up to 38% [20].

6. Conclusion

In lieu of an existing vaccine at the early stages, the large-scale deployment of digital surveillance in general and contact tracing applications, in particular, has been a “beacon of hope” in curbing the pandemic.

While some of these measures are based on advice from epidemiologists and are effective, others may not be. It is essential to keep track of them. Especially that some of these measures have put some of the fundamental privacy principles of many nations to the test. For example, Hungarian governments suspended EU data protection rights in May 2020 to relax the obligation of authorities to notify individuals when collecting personal data while applying containment measures [21].

Although challenges and research gaps concerning security and technology / social constraints are still valid, recent social studies observed that users have felt more comfortable to use contact-tracing applications as the pandemic progresses. But when the pandemic is over, such extraordinary measures must be put to an end and held to account.

References

[1] G. Qiu, Z. Gai, Y. Tao, J. Schmitt, G. A. Kullak-Ublick, and J. Wang. (2020) “Dual-Functional Plasmonic Photothermal Biosensors for Highly Accurate Severe Acute Respiratory Syndrome Coronavirus 2 Detection.” ACS Nano, vol. 14, no. 5, 5268–5277, pMID: 32281785. [Online]. Available: https://doi.org/10.1021/acs.nano.0c02439
[2] G. T. Marx. (2015) “Surveillance Studies.” International Encyclopedia of the Social & Behavioral Sciences, vol. 23, no. 2, 733–741.
[3] A. Izaguirre. (2020) “W.Va. judge allows ankle monitors for virus scofflaws.” [Online]. Available: https://bit.ly/2ZZufrV
[4] R. McArthur. (2020) “Bahrain launches electronic bracelets to keep track of active COVID-19 cases.” [Online]. Available: https://bit.ly/2Wjk04O
[5] O. Hersent, B. Vanaken, and R. Gupta. (2020) "Proximity Detection and Contact Tracking for COVID-19 Webinar." [Online]. Available: https://bit.ly/3erLjzQ
[6] L. Dudley. (2020) "China’s Ubiquitous Facial Recognition Tech Sparks Privacy Backlash." [Online]. Available: https://bit.ly/3j08AFW
[7] BBC. (2020) "Coronavirus France: Cameras to monitor masks and social distancing." [Online]. Available: https://bbc.in/3eu4h8E
[8] J. Walls. (2020) "Covid-19 coronavirus: 89 new cases - highest daily rise yet." [Online]. Available: https://bit.ly/2ZmmUQ
[9] Vodafone. (2020) "Vodafone launches plan to help counter the impacts of COVID-19." [Online]. Available: https://bit.ly/2W/CXz3
[10] Human Rights Watch. (2020) "Mobile Location Data and Covid-19: Q&A." [Online]. Available: https://bit.ly/3058vyN
[11] Deutsche Welle. (2020) "Coronavirus: India's contact tracing app comes under fire." [Online]. Available: https://bit.ly/2AW0qkw
[12] S. Vaudenay. (2020) “Centralized or Decentralized? the Contact Tracing Dilemma.” Cryptology ePrint Archive, Report 2020/531. https://eprint.iacr.org/2020/531, Tech. Rep.
[13] W. H. Organization et al. (2020) “Ethical Considerations to Guide the Use of Digital Proximity Tracking Technologies for Covid-19 Contact Tracing: Interim Guidance, 28 May 2020.” World Health Organization, Tech. Rep.
[14] M. Kassab, and G. Destefanis. (2021) "Blockchain and Contact Tracing Applications for COVID-19: The Opportunity and The Challenges." The 4th International Workshop on Emerging Trends in Software Engineering for Blockchain in conjunction with 28th edition of the IEEE International Conference on Software Analysis, Evolution and Reengineering.
[15] A. D’mello. (2020) “Report Reveals Privacy is Taking Back Seat in Global Contact Tracing Efforts.” IoT Now, May 2020. [Online]. Available: https://bit.ly/3jeKFfY
[16] Access Partnership. (2020) “Digital Contact Tracking: A Comparative Global Study.” Available at https://www.accesspartnership.com/digital-contact-tracking-a-comparative-global-study/. Posted on 27th May 2020.
[17] Marketing Technology Insights. (2020) “New Survey Reveals Growing Acceptance Around Covid-19 Contact Tracing and Exposure Notification Apps.” Available at http://tiny.cc/n47asz.

[18] L. Abeler-Dörner. (2020) "Infectious disease experts from Oxford University and Turing Institute estimate that using the NHS COVID-19 contact tracing app averted between 200,000 and 900,000 infections." [Online]. Available: https://bit.ly/3j3ONMx

[19] L. Silver. (2019) "Smartphone Ownership is Growing Rapidly Around the World, But Not Always Equally." https://pewrsr.ch/2TrV7Cr.

[20] M. Tawalbeh, A. Eardley, et al. (2016) “Studying the Energy Consumption in Mobile Devices.” Procedia Computer Science, vol. 94, 183–189.

[21] V. Makszimov. (2020) "Hungarian government suspends EU data protection rights." [Online]. Available: https://bit.ly/2Bhjddi