Contents lists available at ScienceDirect

Technological Forecasting & Social Change

journal homepage: www.elsevier.com/locate/techfore

Towards a new era of mass data collection: Assessing pandemic surveillance technologies to preserve user privacy

Samuel Ribeiro-Navarrete [a], Jose Ramon Saura [b,*], Daniel Palacios-Marqués [a]

[a] Universitat Politècnica de València, Valencia, Spain
[b] Rey Juan Carlos University, Madrid, Spain

ARTICLE INFO

Keywords:
Mass data-collection
COVID-19
User privacy
Data management
Mobile devices

ABSTRACT

Controlling the coronavirus pandemic is triggering a cross-border strategy by which national governments attempt to control the spread of the COVID-19 pandemic. A response based on sharing facts about millions of private movements and a call to study information behavior during the global health crisis has been advised worldwide. The present study aims to identify the technologies to control the COVID-19 and future pandemics with massive data collection from users' mobile devices. This research undertakes a Systematic Literature Review (SLR) of the studies about the currently available methods, strategies, and actions to collect and analyze data from users' mobile devices. In a total of 76 relevant studies, 13 technologies that are classified based on the following aspect of data and data management have been identified: (1) security; (2) destruction; (3) voluntary access; (4) time span; and (5) storage. In addition, in order to understand how these technologies can affect user privacy, 25 data points that these technologies could have access to if installed through mobile applications have been detected. The paper concludes with a discussion of important theoretical and practical implications of preserving user privacy and curbing COVID-19 infections in the global public health emergency situation.

1. Introduction

In the last several months, the COVID-19 pandemic has caused systematic changes in the society and organizational structures (Guy, 2019; Kim, 2020). Surveillance and control of the coronavirus pandemic is triggering a cross-border strategy carried out by governments to try to control the virus (Pan et al., 2020). A response based on sharing facts about millions of private movements and a call to study information behavior during a global health crisis has been advised worldwide (Chakraborty and Maity, 2020). In this context, different visions of the near future where the control of the current and future pandemics can systematically invade user privacy, at least as we knew it until now, have emerged (Paine et al., 2007). This diversity of opinions is explained by the fact that, while the Internet is global, legislation is local (Kavota et al., 2020); therefore, governments and companies that help to control data management are locally responsible for implementing relevant strategies and data collection strategies and regulations (Malhotra et al., 2004).

The concept of mass surveillance emerged the first decade of the 21st century, after the 9/11 attacks in New York and as a reflection of the phobia of possible new terrorist attacks presented by Zuboff (2015, 2019). Events such as 9/11 in New York caused massive surveillance and listening initiatives by the US government (Sinha, 2013). After 9/11, using tools to track user data to protect people from these types of attacks became a new vigilant normality (Kummitha, 2020). Mass surveillance encourages users to understand that these strategies help the authorities to prevent possible social problems (Arya et al., 2019), as the analysis of these data is an opportunity to predict new incidents, such as terrorist attacks, murders, collapses of the system, traffic jams, and so on (Zuboff, 2015). For instance, while numerous previous studies found parallels with the measurement and tracking of coronavirus infections and future pandemics at a global level (e.g., Gerke et al., 2020, Wen et al., 2020)., this kind of tracking can violate privacy of users who use applications to track coronavirus infections.

Therefore, in a study on connected ecosystems, Zuboff (2015) stated that, when chaos reigns in the society, fear among users means that they indirectly agree to share their data with their governments and private companies (Ando et al., 2016; Kavota et al., 2020). Several scholars have referred to this as mass personalization based on the collective sentiment of feeling safe as well as collective intelligence (Balapour et al., 2020: Elia et al., 2020). However, along with the need for safety (Gayness Clark et al., 2009), people also wish to maintain privacy. From this

[*] Corresponding author.
E-mail addresses: joseramon.saura@urjc.es (J.R. Saura), dapamar@doe.upv.es (D. Palacios-Marqués).

https://doi.org/10.1016/j.techfore.2021.120681
Received 3 September 2020; Received in revised form 11 February 2021; Accepted 13 February 2021
Available online 22 February 2021

moment, companies like Facebook or Google began to understand that the use of Big Data could be a source of prediction of user behavior and be used as a tool to increase their income (Vargo and Hopp, 2020).

Insights into users' movement, tastes, and habits, as well as predicting the possibility of understanding their behavior becomes an added value for companies (Kang and Yang, 2020). Several years later, there was the Cambridge Analytica scandal in which it was found that the private professional sphere controlled and predicted the movements of millions of people helped by a social network such as Facebook (Isaak and Hanna, 2018). Later, it was shown that this alliance was used to shape the voting intentions of millions of voters by predicting the way users think, act, and behave in social networks (Venturini and Rogers, 2019).

Under this paradigm, in 2019, Zuboff published the book entitled *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* which revealed how the data obtained from users through their mobile devices indirectly offer governments and large companies an advantage that can be a potential abuse of privacy (Zhang and Wang, 2020). In this surveillance capitalism, data can be massively collected in the new connected society that uses applications for free in exchange for their data (Zuboff, 2019).

This new connected era means that private companies can be controlling the masses without people being aware of it or at least changing their habits (Karas, 2002; Xu et al., 2015). These conclusions were also supported by media activists Edward Snowden or Julian Assange on different occasions (Chadwick and Collister, 2014). In response to privacy threats, several efforts have been made on the global level to regulate the collection of massive data, such as the right to be forgotten, or updates to the legislation related to the protection of data of Internet users, such as the EU General Data Protection Regulation (GDPR) (Mantelero, 2013).

However, there are doubts in the scientific literature about how these datasets are stored, deleted after processing, or if they are converted into anonymized databases (Knijnenburg et al., 2013). On these databases, applying artificial intelligence techniques such as machine learning and data mining, companies can improve their social listening algorithms to predict user behavior, thus improving the products and services of companies that collect this information (Tan and Zhan, 2017).

During the COVID-19 pandemic, with the development of a mobile application to track the coronavirus, Apple and Google have announced solutions for virus control worldwide (Kaashoek and Santillana, 2020). These two companies base part of their strategic development on the analysis and prediction of user behavior by studying their data (Craker and March 2016). This initiative places both companies at the forefront of enhancing the control and surveillance of the COVID-19 and future pandemics worldwide and, therefore, the management of these data.

This situation also give rise to numerous questions, such as "Where does user privacy begin and end?" "When is mass control of user tracking no longer useful?" "Is geolocation the correct technology to control the COVID-19?" "Will 2020 be the start of the new era of massive data collection and the intrusion of surveillance capitalism as a global order?" "What data will these kinds of mobile applications collect, and who will the data be shared with?" "How will this information be used in the future?" "Are there legal policies in place to prevent abuse?"

However, a central question here is as follows: "What are the limits and options that this new era allows from the point of view of privacy and Big Data collection?" Understanding these approximations is important, as the risk of tracking a connected society may cause violations of user privacy. The first step needed to control these surveillance actions is gaining a comprehensive understanding of what data about users are obtained, and how these data can be accessed (Shilton, 2009).

In this way, we now enter a new stage where large companies that collect large volumes of data acquire access to global crowd control and information management (Zhang et al., 2020). Therefore, in the fight against COVID-19, users should be aware of the limits and available options concerning the use of their data in new mass control approaches proposed by governments and private entities (LaBrie et al., 2018).

This new situation may affect the relationship of democracies with large technology companies, as has already occurred in the case of Cambridge Analytica (Isaak and Hanna, 2018). This case taught the world that the ability to combine demographic and psychographic data of users, with their online habits and behaviors, could predict their voting intentions; it also showed that users could be a strategic target of political campaigns. Therefore, these technologies can cause dramatic social, political, and economic changes worldwide (Blair et al., 2017). Taking advantage of the new circumstances that broaden companies' possibilities of monitoring and managing user personal data, the corresponding techniques can be later expanded to other purposes (Blazquez and Domenech, 2018).

As argued by Mennecke and West Jr (2001), we are at a time when informed societies must create and share a legal framework that establishes the benefits of technology for mass data-based surveillance. Public health can be an element of surveillance for the control of COVID-19 and future pandemics, with or without the collection of data over time (Irache et al., 2019). Therefore, the present situation requires an understanding of available options and technologies to stop the spread of this pandemic (Leite et al., 2020).

Therefore, seeking to identify available surveillance options to track the infections generated by COVID-19 using user data, the present study conducts an original Systematic Literature Review (SLR) of previous studies published thus about strategies, technologies, and actions to track and geolocate data from users' mobile devices. The results are then analyzed from the point of view of user privacy.

The two research questions addressed in the present study are as follows:

- RQ1: What technologies based on collecting information from users' mobile devices can be massively used to track COVID-19 or future pandemics?
- RQ2: What privacy risks of mass surveillance actions are associated with each tracking technology in the current emergency situation?

To the best of our knowledge, this study is the first to review relevant scientific literature on the use of user personal data-points in tracking applications of COVID-19. Therefore, the results will provide meaningful insights for governments, public institutions, non-profit organizations, or private companies about how information science works and how massive collecting data from users can provide a better understanding of the new era and of the ways to cope with the COVID-19 pandemic. In this study, the legal status of all reviewed tracking methodologies will be discussed; therefore, governments and companies can use this discussion as a legal guideline to what is legitimate and acceptable from the information management and privacy perspective.

The remainder of this paper is structured as follows. Section 2 outlines the theoretical framework of the present study. The methodology is presented in Section 3. Section 4 reports the results that are further discussed in Section 5. Finally, conclusions are drawn in Section 6.

2. Theoretical framework

Information sciences and appropriate management of public information have been the subject of study on numerous occasions (Jho, 2015; Keith et al., 2016; Buchanan et al., 2007). In the current global state of emergency related to the spread of the COVID-19 pandemic, understanding and discovering patterns that can help to understand human behavior has become a major challenge to control the current situation (Ahmed et al., 2020).

The combination of data from the physical and the online worlds has led to the development of behavioral models that study mobility, society, economy, or culture, as well as the impact that COVID-19 on these areas (Ivanov, 2020). Data related to users' daily life, their modified behavior, and predictions of their movements have led information management to obtain outcomes that help understand large conglomerates of users (Kaashoek and Santillana, 2020).

According to Mulvenna et al. (2000), at present, we live in the period of mass personalization, as users' web page data on the Internet provide rich information about people, including their demographic, psychographic, and lifestyle data. As argued by Arya et al. (2019), digital marketing strategies that analyze Big Data can effectively segment Internet advertising using remarketing technology. For example, live text analysis techniques are applied to the chats in applications such as WhatsApp, Messanger, TikTok, or Telegram and instantly segment advertising in such applications (Rashidi and Vaniea, 2015; Kang and Yang, 2020). Users, regardless of their being aware of it, accept that companies monitor and carry out a keyword research and textual analysis on users' input, e.g., through monitoring of calls to identify keywords that will be used to segment ads (Vargo and Hopp, 2020).

Therefore, in the ecosystem where data segment live advertising has a very high success rates, the sale of massive data to third parties has become one of the businesses of the 21st century (Palos-Sanchez et al., 2019). However, while beneficial to companies, these practices sometimes violate user privacy.

Similarly, Zhang et al. (2020) investigated data management by public organizations and institutions concluding that the main characteristics that must be followed for information management are truthfulness, transparency, and speed in the management of the information collected (Stamoulis et al., 2001).

Information management in the state of emergency becomes No. 1 priority for institutions that aim to solve the problems faced by the society (Jin et al., 2014). Appropriate management of the information and data linked to it are key elements for the development of communication protocols that respect user privacy and that respond to the needs of health or social crises (Saura et al. (2021)). Therefore, appropriate information management must be analyzed from both user privacy and information acquisition and control perspectives (Wang et al., 2020).

In this context, it is essential to understand which technologies can help collect data from mobile applications, smartphones, and connected devices. Each of these technologies can provide information for companies and institutions to make decisions regarding traceability and the level of information collected, both for monitoring COVID-19 and for future pandemics. The sources of data and the level of sophistication of the mobile technologies used to track users and obtain information is a prerequisite of the development of appropriate strategies that respect user privacy (Rashidi and Vaniea, 2015).

2.1. Mass data-collection through mobile devices

One of the most used ways to collect massive data is through the Internet (Qi et al., 2020), mobile applications (Salo and Makkonen, 2018), and geolocation (Luceri et al., 2018). Mobile applications are small systems installed on users' smartphones that perform specific tasks (Libaque-Sáenz et al., 2020). To install such application on their mobile devices, users must accept the privacy policy and terms of use of these applications. Privacy policy terms should specify how the data will be handled, who will have access to them, which part of the data will be accessed via an application, who the data will be shared with, and whether the data will be sold to third parties or destroyed it (Choi et al., 2018; Fengzhe et al., 2011).

Furthermore, these policies must inform users of the exact management of the collected data, as well as the technology used to obtain the information. If these policies do not appropriately report the use of the data, users' right to privacy may be being violated (Kelley et al., 2012).

The databases and terms of quality and sophistication of mobile data collection and treatment technologies should provide sufficient detail on the following aspects of the data collection process: (i) security; (ii) destruction of the data; (iii) voluntarily access to the data; (iv) time-span of storing the data; and (v) storage (see Table 1).

Table 1
Main characteristics of the data collection processes.

Characteristics	Description
Data privacy	Level of data which the application will have access to. Personal data such as age, gender or gender, among others. Anonymous use of these data and indication of the management to third parties.
Data security	Level and quality of implementation of application security against possible attacks that may steal data collected by the application. There are security level protocols to evaluate the management of user data.
Data destruction	Time span during which the data will be stored on servers of private companies or public institutions that collect the data. The deletion of the data must be certified anonymously, and users should be informed who would have access their data before they are deleted.
Voluntary access	There must be protocols that indicate whether the collection of their data through an application is voluntary or mandatory for its use. The data that the application collects must be specified so that users voluntarily accept the said collection.
Time span	The frequency with which the data are collected. Ranges from weekly or monthly to real-time data. The latter allows the automatic management of data with the use of AI applications.
Storage	The type of data storage. The data can be stored on a server or be part of the software that users use to access services on the Internet, such as cookies or the cache of browsers and applications. The user must be informed if these data should be deleted by him/herself or by companies within the indicated time frame.
Technology	Technology used to access and collect user data. Depending on the sophistication of the given technology, the speed of data collection and the amount may be truncated.

Source: The authors.

Once the characteristics of data collection and its relation to user privacy are specified, it is essential to understand the purposes of using the collected data. Accordingly, the privacy of the data must be defined based on the nature of the data (Suganya, 2018). The data are typically classified according to the information they provide about users (Irache et al. (2019)). In this respect, four types of data are distinguished (Taylor (2017); Schobel et al., 2020) (see Table 2).

Under these specific characteristics of the type of technology for data collection and the nature and characteristics to which the applications that have access to these data must respond, this study uses an SLR to identify technologies that, based on these characteristics, allow for tracking COVID-19 infections and preventing the growth of possible future pandemics based on the monitoring of user data.

Table 2
Privacy levels according to type of data collection and user privacy.

Characteristics	Description
PII	Personally identifiable information, or PII, is the data set that can be used to identify, contact, or locate a user. It is also the data set that allows one to differentiate one individual from another.
PHI	Personal health information, or PHI, is the data related to the medical history information of a user or individual. It is also the set of information collected from medical sources and health treatments that can identify a user.
PIFI	Personally identifiable financial information, or PIFI, is related to the collection of information in financial and accounting terms, such as credit cards, bank accounts, and their details and other data that affect the economic health of the individual.
SR	Educational (Student) records, or SR, are the set of data that identifies the level of training of a user, as well as individual's grades, transcripts, billing details, and other educational records. These data may segment the user and his/her interests.
Non-sensitive PII	It is a set of information that is already in the public domain and, therefore, is not sensitive to the user. However, if it is combined with PII, it can offer information about the user or individual.
Non-PII	Non-personally identifiable information (Non-PII) is data that cannot be used in any way to identify a person. The most common examples are the ID of the connected devices, cookies, or the like. However, both types of information may offer clues as to who the user or individual is.

Source: the authors.

3. Methodology development

The methodology developed in this study is the Systematic Literature Review (SLR). The SLR aims to answer the research questions addressed in this study (Wang et al., 2019). For the development of the methodology, we followed previous studies, such as Webster and Watson (2002) and Stieglitz et al. (2018). Our overarching aim was to present the theoretical framework linked to the proposed objectives and structuring the searches that will be carried out to cover the gap in the literature on an emerging and original research topic.

The SLR methodology is an apt tool for the studies that aim to analyze emerging issues or problems that could benefit from the study of important theoretical concepts proposed in the literature (Bem, 1995). The study of these theoretical concepts would provide new findings that can define the questions posed. As argued by Saura (2020), the emerging field of massive data collection applied to the COVID-19 and future pandemics will benefit from a logical conceptualization of the application of these kind of technologies in the new digital era.

To develop the methodology, we followed Stieglitz et al. (2018) and Saura (2020) and divided the SLR into the following three steps. The first step was based on the analysis and definition of the main theoretical concepts. In the present study, this included the classification of the main massive data collection techniques used in the literature. To this end, we followed Bem (1995) and Webster and Watson (2002) who argued that "*a coherent review is born only from a conceptual coherent structuring of the topic itself*".

Focusing on our research questions, we used the SLR to analyze the application of techniques, experiments, and methods used to track user information based on the current situation worldwide. In this way, and following Saura (2020), we identified and classified the main contributions of the literature in relation to the theoretical framework. In the second part of the methodology development, the literature was analyzed in depth to identify the studies that analyzed relevant issues and technologies to collect data from mobile devices. This phase allowed us to inductively synthesize prior research and group them based on basic concepts and definitions (Stieglitz et al., 2018).

Finally, in the third phase, the main contributions of the literature were analyzed to identify technologies to collect data from mobile devices. This included highlighting the main techniques, experiments, and methods used to track user information, as well as pertinent theoretical and privacy frameworks.

To finish with the SLR, we reviewed the studies by vom Brocke et al. (2009), Brocke et al. (2015), and Stieglitz et al. (2018) where predefined and selected terms were searched in the databases regarding indicators such as Title, Abstract and Keywords. At this point, all irrelevant studies were removed from the results.

The search terms were chosen to identify the main techniques, experiments, and methods to track user information. The results were classified by categories and filters (e.g., Technical, Theory, Privacy, Experiment and Method). Furthermore, only original articles and reviews were analyzed. Proceedings, books, chapters, or magazines were excluded from the SLR process. The queries in the databases (see Table 3) were performed on April 5 and 8, 2020.

As mentioned previously, the present study is database-oriented and took into account all articles published and indexed in the scientific databases, including ACM Digital Library, AIS Electronic Library, IEEE Explore, ScienceDirect, and Web of Science. The detailed list of the terms used is provided in Table 3.

In order to identify in potentially relevant articles, the papers' titles, abstracts, and keywords were examined in depth. Relevant research studies were defined as papers that identified the main techniques and approaches to track user information during the COVID-19 and other pandemics. Accordingly, in the article selection process, we did not focus on the type of analysis or methodology used in a particular study.

Finally, the articles identified as relevant were classified based on different definitions, theoretical concepts, and application methods regarding the importance of mass data collection processes. Following Moher et al. (2009), Brocke et al. (2015), and Stieglitz et al. (2018), the articles with inadequate terms and inconclusive results, no relation to the research topic, as well as without quality evaluation or description and specification of terms were excluded.

In this way, the total number of articles identified based on each of the objectives proposed in the SLR process was as follows: ACM Digital Library, 22 relevant results of 402 total results; AIS Electronic Library (9/27); IEEE Explore (9/285); ScienceDirect (17/344); Web of Sciences (16/159). Overall, the total number or results was 1217 articles, of which 73 were classified as relevant.

The studies identified as relevant in the search process were categorized and classified based on their main focus. Specifically, if a study focused on a data-collection technique, it was classified as related to the collection of information using different methods. Second, the articles on privacy concerns were classified based on user information rights and access to control user information. A third group of articles that focused on the review of methods, techniques, and experiments was analyzed from a broader perspective. The five categories used in classifying the reviewed studies are outlined in Table 4. The results of the SLR process are summarized in Table 5.

In addition to the literature review process, we also performed the HOMALS analysis using SPSS (v20) software for each group of keywords found in the articles. HOLMAS is a well-known method of multiple correspondence analysis (MAC) procedures to analyze qualitative data (Kiessling et al., 2019). Specifically, it is an exploratory analysis process for the elaboration of graphical display of multivariate categorical data.

HOMALS results allow researchers to identify relationships between dichotomous variables (see Gonzalez-Loureiro et al., 2015). Specifically, the HOMALS analysis allows a value of "1″ to be entered when the keyword is found in relation to a subject, and the value "0″ otherwise.

In this way, the outcome of this process is a proximity map where, through the analysis of keywords, the proximity between different approximations between the two axes can be categorized (Kaciak and Louviere, 1990).

In this map (see Fig. 1), the center corresponds to the average position of the articles within the subject, in which smartphones, mobile devices, and surveillance technologies have a greater approximation to the rest, which allows researchers to understand that the smartphones and mobile devices are the main tools used to collect user data.

Table 3
Search terms used in the SLR.

Search terms			Data Bases	Fields
data collection OR data-collection* OR mass data collection*	AND	mobile devices OR app OR smartphone OR location	ACM Digital Library AIS Electronic Library IEEE Explore ScienceDirect Web of Sciences	Title, Abstract Keywords

* These terms were only used when the search of the terms.
"data collection" AND "mobile devices" did not obtain the expected results.
Source: The authors.

Table 4
Categories used in article classification.

Article classification	Description
Technical	Technical process to study a data-collection technology
Theory	Theoretical framework of a data-collection technology
Privacy	Analytical focus on technology privacy
Experiment	The experimental perspective on a data-collection technology
Method	The method used to develop a data-collection technology used and collect data has been analyzed

Source: The authors.

Table 5
Relevant papers found in the Systematic Literature Review (SLR).

Authors	Journal	Category	Main focus in SLR				
			Technical	Theory	Privacy	Experimental	Method*
Allmendinger et al. (2017)	Journal of Structural Geology	Geology		●	ϕ		○
Aloi et al. (2007)	IEEE Transactions on Instrumentation and Measurement	Electrical & Electronic Engineering					○
Ando et al. (2016)	IEICE TRANSACTIONS on Information and Systems	Computer Sci. & Information Systems	●		○		ϕ
Arriagada et al. (2018)	Journal of Intelligent Transportation Systems	Transport. Science & Technology	○				●
Beigi and Liu (2020)	ACM Transactions on Data Science	Computer Sciences & Information System		●	○		
Ben-Gal et al. (2019)	ACM Transactions on Knowledge Discovery from Data	Computer Science		○			●
Cabalquinto et al. (2020)	Telematics and Informatics	Information Science & Library Science		○	●		
Can and Demirbas (2015)	Journal of Network and Computer Applications	Public, Environmental & Occu. Health	○				●
Cao et al. (2010)	Proceedings of the VLDB Endowment	Computer Science	●	○			ϕ
Chai and Nayak (2018)	Electronic Journal of Statistics	Statistics & Probability				○	●
Chandra and Sudarshan (2017)	Proceedings of the VLDB Endowment	Computer Science	○			ϕ	
Chen et al. (2012)	Communications of the Association for Information Systems	Information Systems		○			
Cheng et al. (2018)	IEEE Internet of Things Journal	Information System & Management		○			
Choi et al. (2019)	Journal of Public Economics	Economics and Econometrics		○	●		
Choi et al. (2018)	Journal of Public Economics	Business & Economics		○	●		
Dimitriou and Krontiris (2017)	Journal of Network and Computer Applications	Computer Science Applications	○		●	ϕ	
Giroux et al. (2019)	Environmental Modelling & Software	Environmental Science	○				●
Gogus and Saygın (2019)	Heliyon	Multidisciplinary		●	○		ϕ
Grover (2013)	Digital Investigation	Computer Science Applications		○	●		
Guo and Ma (2017)	IEEE Access	Computer Science		○			
Ho et al. (2015)	Pacific Asia Journal of the Association for Information Systems	Computer Sciences & Information System		○			ϕ
Hsieh et al. (2014)	ACM Transactions on Intelligent Systems and Technology	Artificial Intelligence		○		ϕ	●
Hu et al. (2010)	ACM Transactions on Database Systems	Information Systems	●	○			
Irache et al. (2019)	BMJ Global Health	Public, Environmental & Occu. Health		○			●
Jin et al. (2018)	Procc. ACM on Interactive, Mobile, Wearable & Ubi. Tech.	Engineering	○		●		
Keith et al. (2016)	AIS Transactions on Human-Computer Interaction	Computer Sciences Applications		○	●	ϕ	
Khan et al. (2019)	Future Generation Computer Systems	Computer Network & Communications		●	○		
Kim and Jang (2019)	IEEE Communications Letters	Telecommunications	○		●	ϕ	ϕ
Lee and Tsai (2014)	ACM Transactions on Multimedia Computing, Comm., and Appli.	Computer Networks & Communications		○		ϕ	●
Lesani and Miranda-Moreno, 2019	IEEE Transactions on Intelligent Transportation Systems	Computer Science Applications	○				ϕ
Li et al. (2015)	Science China Information Sciences	Computer Sci. & Information Systems	●			○	ϕ
Li et al. (2015)	IEEE Transactions on Computers	Computer Science		●	○	ϕ	
Libaque-Sáenz et al. (2020)	Information & Management	Information Systems & Management		●	○	ϕ	
Liu et al. (2019)	Procc. ACM on Interactive, Mobile, Wearable & Ubi. Tech.	Engineering			○	ϕ	●
Luceri et al. (2018)	Pervasive and Mobile Computing	Computer Science	○		●		ϕ
McKenzie and Slind (2019)	Applied Geography	Social Sciences	○	●			
Mokbel et al. (2016)	Proceedings of the VLDB Endowment	Computer Science	●		○		
Mun et al. (2014)	ACM Transactions on Sensor Networks	Computer Networks & Communications		●	○	ϕ	
Nguyen (2020)	Internet of Things	Internet of Things Applications	●	○			
Perentis et al. (2017)	ACM Transactions on Internet Technology	Computer Networks and Communications		○		●	
Qi et al. (2020)	Information Fusion	Information Systems	●	○			
Ravenscroft (2017)	Journal of Computing Sciences in Colleges	Computer Science		○			
Robertson (2019)	Common Market Law Review	International Relations		○	●		
Sajjad et al. (2019)	Computers & Security	Computer Sci. & Information Systems	○		●		ϕ
Sajjad et al. (2019)	Computers & Security	Computer Science		●	○	ϕ	
		Information Systems		○			

(continued on next page)

Table 5 (*continued*)

Salo and Makkonen (2018)	Communications of the Association for Information Systems						
Sang et al. (2017)	ACM Transactions on Intelligent Systems and Technology	Artificial Intelligence		○		●	
Schobel et al. (2020)	International Journal of Environmental Research and Public Health	Public, Environmental & Occu. Health	○			●	
Silva et al. (2019)	ACM Computing Surveys	Computer Science		○			
Spolaor et al. (2017)	IEEE Transactions on Mobile Computing	Computer Network & Communications	○	○			
Steenbruggen et al. (2015)	Telecommunications Policy	Information Systems		○			
Stills et al., 2020	AIS Transactions on Human-Computer Interaction	Computer Science	●	○		ϕ	
Taylor (2017)	Politics, Philosophy & Economics	Ethics and Political Science			○		
Terlizzi et al. (2019)	AIS Transactions on Replication Research	Computer Sciences		●	○		
Tuunanen et al. (2006)	Journal of Information Technology Theory and Application	Computer Sciences & Information System	○	●			
Vankipuram et al. (2017)	Computer Methods and Programs in Biomedicine	Computer Science Application Software	○				●
Wang and Zhang (2016)	IEEE/ACM Transactions on Networking	Computer Science Applications		●	○		ϕ
Wang et al. (2016)	ACM Transactions on Multi. Computing, Comm., and Appl.	Computer Networks and Communications	●	○		ϕ	
Wang et al. (2018)	IEEE Access	Computer Science		●	○	ϕ	
Wang et al. (2018)	ACM Transactions on Sensor Networks	Computer Networks and Communications		○	●		ϕ
A. Wang et al. (2019)	Digital Communications and Networks	Computer Network and Communications		●	○		
Wilson and Djamasbi (2019)	Communications of the Association for Information Systems	Information Systems	○	○			
Wu et al. (2017)	ACM Transactions on Intelligent Systems and Technology	Artificial Intelligence	○				
Xu et al. (2015)	IEEE Journal of Selected Topics in Signal Processing	Engineering		○	●		
Xu et al. (2016)	Geospatial Health	Public, Environmental & Occu. Health	○			●	
Yang et al. (2019)	IEEE Transactions on Vehicular Technology.	Engineering				○	●
Yao et al. (2015)	IEEE Transactions on Information Forensics and Security	Computer Networks and Communications		○			
Yaqub et al. (2020)	Digital Government: Research and Practice	Information systems, Law	○				●
Yu et al. (2016)	ACM Transactions on Knowledge Discovery from Data	Computer Science					○
Zhang et al. (2016)	Computer Networks	Computer Networks and Communications			○		●
Zhang et al. (2009)	Communications of the Association for Information Systems	Information Systems		○			●
Zhou et al. (2018)	Procc. ACM on Interactive, Mobile, Wearable & Ubi. Tech.	Engineering		●	○		ϕ
Zhu et al. (2016)	ACM Transactions on Knowledge Discovery from Data	Computer Science	○	●		ϕ	

○ Research article main topic analyzed.
● Secondary focus on which the article has been analyzed.
Ø Analysis approach for sub-theme analyzed in the same article (methods).
* When an article is classified as an experiment, the method may or may not be analyzed, because sometimes the experiment may or may not represent a monitoring strategy for pandemic systems or user location.
Source: The authors.

In addition, different categories of keywords divided into the types of methodology approach used in the reviewed articles were defined. As explained above in the description of the literature review process, these included technical, theoretical, experimental, and data-based methods.

A group of keywords was also identified in relation to mobile devices. Finally, groups of keywords focused on the analysis of data collection approaches.

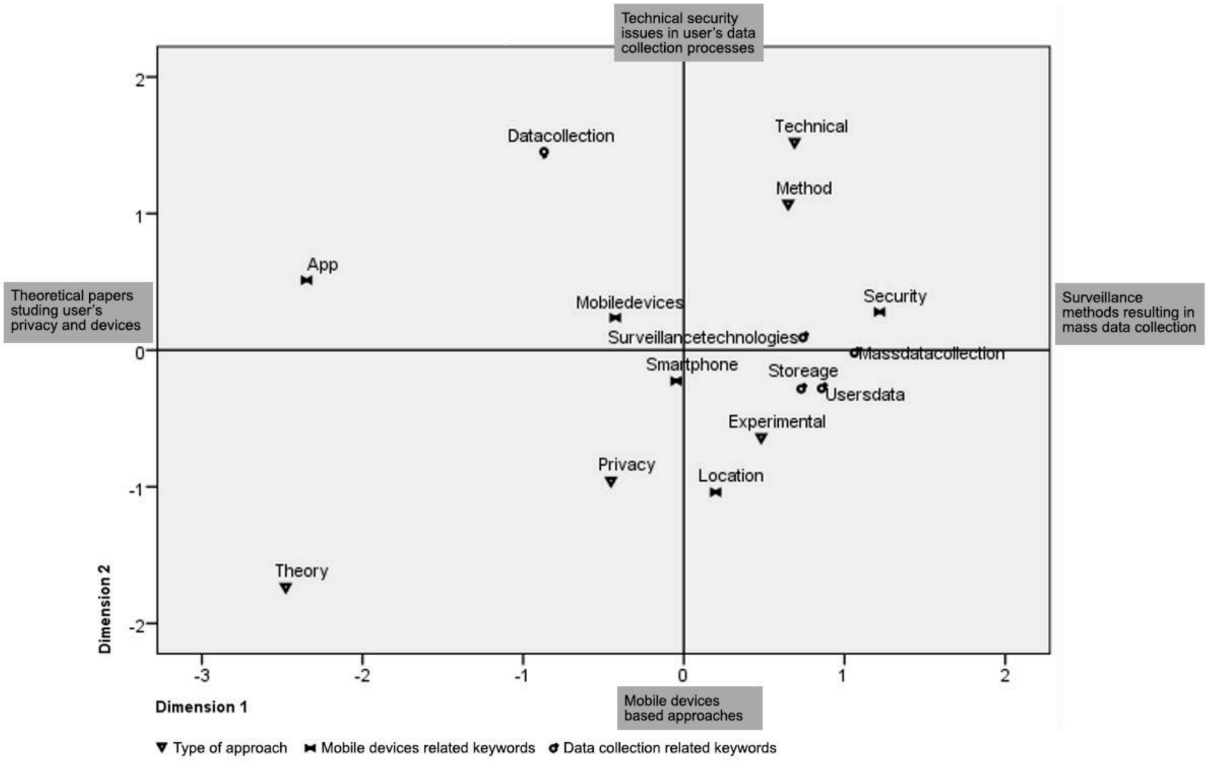
Regarding the indicators identified using the HOLMAS approach, it should be highlighted that Dimension 1 has an eigenvalue of 0.122 and dimension 2 of 0.116. The eigenvalue measures how much of the categorical information is explained by the variance (Kaciak and Louviere, 1990; Gonzalez-Loureiro et al., 2015). In our results, Dimensions 1 and 2 accounted for 12.2% and 11.6% of variance, respectively. The largest possible eigenvalue for each dimension is 1. It should be understood that two dimensions together provide an interpretation in terms of distances (Kiessling et al., 2019).

The key concepts of keywords are close to each other because they belong to the same category. Categories of different variables would be closer if they belong to the same objects. The distance from a keyword to the origin reflects variance from the "average" response pattern.

This average response pattern corresponds to the most frequent category for each variable (Kiessling et al., 2019). Keywords with many characteristics corresponding to the most frequent categories lie near the origin. In contrast, keywords with unique characteristics are located far from the origin.

4. Results

Using SLR, a total of 13 data collection and surveillance technologies (see Table 7) have been identified. Furthermore, the technical characteristics of each technology for mass data collection were identified (see Tables 6 and 7). Next, the classification of location-based services work used by each specific technology (see Table 8) was used. Finally, the main data collected from user mobile devices for mass surveillance were



Source: The authors

Fig. 1. Results of the HOMALS analysis.

Table 6
Classification elements for the identified technologies.

Characteristics	Description
Security	Cloud (CLO), Tokenization (TO), Data Classification (DC), Multiple-Factors Authentication (M-F)
Destruction	Overwriting (OV), Degaussing (DE), Physical destruction (PD)
Voluntary access	Optional (OP), Required (RE), Compulsory (CO)
Time span	Real-time data (RTD), Batch Processing (BP)
Storage	Local (LO), External (EX)

Source: The authors.

identified (see Table 9).

4.1. *Data-based technologies characteristics to monetarize pandemic symptoms tracking user's mobile devices*

With regard to user privacy, all reviewed data-collection technologies had their pros and cons. Each of the reviewed technologies was classified according to the following aspects of the data-collection process (a) security of the data; (ii) destruction of the data, (3) voluntary access to the data; (4) time span of data collection and, (v) storage of the collected data (see Table 6).

In relation to security, we classified cloud technology where data are sent and stored remotely in the cloud (i.e. servers belonging to private companies or institutions); tokenization that refers to instances when additional security is applied to the data so that they are non-sensitive or anonymized; and multiple-factors authentication that focuses on the application of an additional security protocol for data access, e.g., access to various hardware points to authenticate the user.

With regard to destruction, here classified overwriting has been identified, i.e. the process of replacing old information with new information. This process is automatic for data storage and is considered part of the data destruction, since, in principle, the old information is removed. Furthermore, degaussing is a process that guarantees that information is no longer retrievable; therefore, degaussing involves reducing and eliminating unwanted data stored on laptop or hard drives. However, this process does not allow information to be re-stored on the same storage device.

Physical destruction refers to the physical removal of the hardware where the information is stored. It is an expensive option that is sometimes used by companies to remove sensitive information (Svantesson, 2015). As concerns voluntary access, here it was classified as optional (i. e. obtaining of information is based on optional adjustments for the user) and required (i.e. when using an application that uses this technology requires access to the data). Another type of voluntary access is compulsory, which includes technologies or applications that cannot be used or installed without generating access to the data; in such cases, granting access to user data is compulsory.

With regard to time span, here classified real-time data was defined, i.e. process of obtaining data in streaming as well as the analysis and collection process generated in real time (Saura et al., 2019). Another type was batch processing, which refers to the collection of data from batch to batch, i.e., the data are first collected by the user and then by the technology.

Finally, regarding storage, local or external options were identified. In the former, the user can delete the stored information, while, in the latter, companies or institutions with access to data are responsible for storing them in their facilities that are external to the user's device. Accordingly, with external storage, user data can be sold to third parties, as specified in the terms of use.

Based on this classification, Table 7 presents a description of the 13 technologies and data sources that can be used to collect user data.

4.2. *Located-based user classification services*

Using the SLR methodology, relevant technologies that could also be used for the development of strategies for surveillance and monitoring of

Table 7
Technologies to track pandemics symptoms tracking user's mobile devices.

Technology	Description	Security	Destruction[1]	Voluntary Access	Time span	Storage
Location	Location-based services (LBS) use real-time data (RTD) and geo-data from a mobile device or smartphone to provide information.	CLO / DC	OV / DE	RE	RTD	EX
Bluetooth	It is a standard for the short-range wireless interconnection of mobile phones, computers, and other electronic device that can share information, documents, images and other files.	TO / CLO	OV / DE	RE	BP	EX
GPS	Global Positioning System (GPS) is a radio navigation system that uses radio waves between satellites and a receiver inside smartphones to provide location and time information.	DC / TO	OV / DE	RE	RTD	LO / EX
External API	Third party applications can join external APIs like Apple and Google are developing worldwide. It lets iOS and Android software communicate with each other over Bluetooth technology, allowing developers to build a contact tracing app that will work for both.	TO / DC	OV / DE	RE	RTD	EX
DP-3T	It is a decentralized privacy-preserving proximity tracing. DP-3T is an open-source protocol for Bluetooth-based tracking where an individual phone's contact logs are stored only locally, so no central authority can know who has been exposed.	DC / M-F	DE / PD	OP / RE	BP	LO
ID Network Location	The ID network is a mobile virtual provider individually per one smartphone. This ID can be tracked using provider data.	DC / TO	OV	CO[2]	RTD	EX
Textual Analysis	It consists of the analysis of keywords found in conversations in mobile applications and publications on the Internet and that can segment advertising, send notifications on specific topics, and listen to user conversations.	DC	OV	RE	RTD	LO
Logbook systems	It is a computer-based software program for recording (logging) states, events, or simply conditions used for complex machines.	DC / TO	OV / DE	OP	BP	LO
Meta data	Meta data provide information about other data such as descriptions, interests, behaviors or details about the user who is surfing the Internet.	DC	DE	CO	BP	LO
Data Logging	Automatic Location Communicators (ALC) automatically log data through positioning and communications technology. They allow for remote observation through recording.	CLO / DC	OV / DE	OP	RTD	EX
Online Tracking	When users access a web page, they create data related to psychographic, behavioral, geographic and lifestyle indicators. These can be remotely monitored.	CLO / DC	OV	RE / CO	RTD	LO
Third-party sources	Third-party data can be used to from data aggregators to expand a dataset. Data aggregators are used to increase the quality of data from different sources of information.	CLO / DC	OV/ DE	OP	BP	LO
Mobile Crowd-sending (MCS)	It is a technique where a group of users with mobile devices collectively send and analyze data to share information to measure, map, or predict actions.	CLO / TO / DC	OV	OP	BP	LO / EX

[1] If it does not depend on the user, the destruction of the data by third parties is usually based on OV or DH. PH can be used when the user him/herself can destroy his/her storage device.

[2] There is no option to use a terminal connected to the coverage system and the Internet without being assigned an ID Network Location.

Source: the authors.

Table 8
Location-based classification terms found in SLR.

Term	Description
LBSN	Location-based social networks are social networks that use features such as GPS or similar to broadcast the user location in stream. These networks can be mobile applications or web apps.
LBS	Location-based services are software services that use geographic data and user information and that may or may not be applications.
LBMS	Location-based mobile services focus on using the geolocation of a device (e.g., a smartphone or any other connected device) to provide the trace of the location information of the user who uses this device.

Source: The authors.

symptoms of COVID-19 or future pandemics have been identified. For instance, approaches such as local differential privacy (LDP), a state-of-the-art approach in statistical computer sciences, and statistically segmented databases can help increase user privacy. Therefore, companies should focus on using these types of statistical models to increase the privacy of their massive data collection processes. For example, there is also the (alpha, k) -anonymity, a widely used privacy-preserving model that is effective for protecting individual privacy before microdata are released.

In addition, the development and use of new connected devices, such as the Internet-of-Things (IOT) or 5 G technology, gives rise to new aspects and concerns regarding user privacy (Bresciani et al., 2018). These new technologies offer innovative data collection solutions and increase streaming capacity. The appearance of such technologies in application development on international level presupposes the existence of rigorous regulations concerning their application in data-collection endeavors.

In this context, user location has become a leading indicator of the data that can tackle a pandemic or help companies and institutions monetize user tracking. Therefore, location is the key to understanding the services focused on user location.

The results of our review suggested that relevant practices of identifying user location can be broadly categorized into the following three groups (see Table 8): (1) location-based social networks (LBSN); (2) location-based services (LBS); and (3) location-based mobile services (LBMS) (see Table 5 for their definitions).

4.3. *User privacy and mass surveillance*

Using the identified technologies to track user location and movement can encourage the creation of the so-called behavior-based segments of users that can further be employed by companies to predict users' actions, location, content consumed, use of physical facilities, and so on.

With regard to privacy, the issue here is not the very fact of a user's accepting one technology or another, but the predictability that companies achieve with the analysis of the data collected applying data-mining techniques and identifying patterns that segment users.

If the activities of mass surveillance are complemented by social listening, i.e. monitoring users' actions and content they publish on social networks, the ability to predict users' habits and behaviors can become very high. This analysis can also be complemented with the analysis of the content created by users, also known as user-generated content (UGC) (Reyes-Menendez et al., 2019).

Table 9
User data points accessible through mobile applications.

Data	Description
Age	User age based on the content they enjoy and the type of media consumed on the terminal.
Gender	User gender based on the applications and content they enjoy on the terminal.
Location	Access to user location through GPS applications or geolocation access points.
Household income	User income level based on the analysis of purchases made and bank applications by social class.
Marital status	User marital status based on contact lists, social media statuses, or emergency contacts.
Family size	User family size based on subscriptions to family platforms or activation of user-safe browsing.
Interests	User interests based on the type of installed applications, browsing history, messages sent through chats, etc.
Preferences	User preferences for the A / B test comparison of decisions made in the device.
Opinions and commenting	User opinions through the analysis of applications intended for this use and textual analysis techniques on product reviews or email meta data.
Browsing history	User browsing history based on the identification of the main sources of information or categories of sites visited.
Purchase history	User purchase history and categories of purchases made (retail, alcohol, sports, health, etc.
Social network use	Type of social networks used, time of use, and type of use.
Ad interactions	User interaction and engagement with advertising banners and percentage of return on investment of each user
Newsletter sign-ups	Type of subscriptions to which the user is registered
Types of media being consumed	Type of media content consumed on the device.
Search terms used	Words used in search engines; identification of patterns of user behavior.
Bank company	User bank account based on the analysis of banking applications installed on the device.
Sports	Type of sport based on interests, consumed media, and installed applications.
Nearby cell phone towers	Analysis of the phones with which a user has been in contact by messaging, Bluetooth or other networks
Nearby Wi-Fi routers	User location identification based on the Wi-Fi points to which the terminal connects automatically.
Music liked	Accessing application information to listen to music or to files saved on the device
Level of education	Analyzing applications related to the university education sector, educational techniques, professional field, and so on.
Health information	If a user has an illness, based on the type of mHealth app that s/he uses to control symptoms and carries out treatment, s/he can give information about symptoms or habits.
Political ideology	User political ideology depending on the type of newspaper applications installed or the browsing history of these websites.
Photos	Many applications request information from the terminal images to be shared with other users. The use and access of this must be monitored.
Text messages	Photos are a source of information regarding promotions and newsletter subscriptions. Text messages can be used to obtain account verification and for payment information. Test messages also provide information about the email account or the bank card used.
Microphone	Many applications request information from the microphone in order to make audio notes or recordings. Sometimes these applications segment advertising based on active listening in the background.

Source: The authors.

These actions can be applied not only to user data, but also extend to the markets. For example, data analysis techniques can be used to identify trade patterns, which can provide an overview of the types of products and services that a country is trading. If the monitored products are health and symptom care items related to medical treatment, the outcomes of such analysis can also determine the degree of severity of the disease, such as the current COVID-19 pandemic, in a given country or continent.

The results of using the SLR method allowed us to identify the following user data points accessible through mobile applications (see Table 9).

5. Discussion

This study focused on identifying which technologies can be used to collect information from user mobile devices with the aim of tracking COVID-19 or future pandemics. We also explored the privacy risks of mass surveillance actions associated with each tracking technology identified in the current emergency situation.

Under this premise, we found that the applications installed on mobile devices are sources that motivate users to enjoy content and share information. However, as argued by Libaque-Sáenz et al. (2020), these applications can be used by companies to predict and understand user behavior.

In the present study, 13 technologies that can help to not only track users' location, but also offer actionable insights on the COVID-19 pandemic for governments and public institutions were identified. The information collected using such technologies—particularly, and the identified data—underscore the importance of user privacy in this connected era.

Of note, technologies that use famous applications have become commodities for most users, and these technologies are used in free applications (Rashidi and Vaniea, 2015). These freemium models are based on offering a free application that collects user data, in exchange for the almost free use of the services offered by the application. If the user wants to upgrade to the premium model, s/he has to pay.

However, it should be noted that more information about users translates into more possibilities to predict user behaviors (Kang and Yang, 2020). On the one hand, this can increase the ability of governments to quickly detect the symptoms of COVID-19 and other pandemics; on the other hand, if the collected information is not treated appropriately, this can violate user privacy.

Overall, the use of various data collection technologies and collective analysis can be used massive behavioral modification where users are recommended not to visit a place due to a higher risk of contagion. In fact, it is with this objective that many national governments and large corporations, like Apple and Google, have launched many tracking initiatives.

Similarly, the analysis of these applications based on the identified technologies will become the source for behavior-based segments that companies can use to develop strategies to predict user behaviors based on artificial intelligence (Hermalin and Katz, 2006).

Privacy is a critical concern for users, as, whenever users agree with the terms of use when installing an application, their information can be sent multiple times to third parties. There have also been concerns about transparency in this area (Ando et al., 2016). Normally, users use applications on a daily and free basis to feel integrated in the digital society and do not pay attention to the details of the terms of use and privacy policies (Steinfeld, 2016). Can this issue be related to the lack of appropriate education of users about possible maltreatment of their personal data? And should education on the treatment of user personal data be improved?

The results of the present study question the integrity of the system characterized by massive collection of Big Data. For instance, should all users have a digital life and use digital technologies? If someone does not have a smartphone, will s/he be out of the control of COVID-19 and, therefore, separated from the rest of the users? Consequently, is this new digital era creating a new form of social inequality based on the use of digital technologies? The 13 technologies identified as well as their characteristics, depend on users' having a connected device or a mobile through which they can be tracked.

Furthermore, while the identified information collection and tracking technologies target the users, they do not help users solve their problems or to track their symptoms. Therefore, the data that can be collected from users can help identify not only the current location of users, but also their future movements, allowing governments to anticipate users' actions to prevent possible contagion. From the technical point of view, it is an efficient process; however, from the point of view of the privacy of the users, doubts arise about whether such surveillance is legitimate (see Moore, 2011; Koshimizu et al., 2006). The standardization of the rules for monitoring and controlling users data, anonymized or not, must be carried out at a global level (Jensen et al., 2005), as the Internet is a global technology so local regulation would not affect the privacy of user data.

The results of the present study suggest, for the sake of user privacy, there should be a requirement to delete all collected data after 30 days and to provide evidence about this deletion. The technologies used to track COVID-19 infections must follow quality protocols based on security and temporality of data collection so as not to invade user privacy. Users should also be given the right use applications sporadically, rather than mandatory, and have the possibility to freely install or uninstall an application.

In reality, however, the application industry makes money from applications because of the data they collect (Lambrecht et al., 2014). Therefore, companies often integrate third-party libraries that allow these external entities to push ads and other content on their mobile applications. These facts must be suitably studied and monitored, since the types of applications and technologies chosen to pursue users with symptoms of COVID-19 and other diseases must be perfectly free from the objective of selling data to interested third parties in order to obtain economic benefit (see Shafer et al. (2005) and Langley et al. (2020)).

In the present-day digital age, there are numerous data sources (smart cities, cars, smart homes, voice assistants, smart clothes, health devices, face recognition systems, etc.) (Scuotto et al., 2016) that can predict user behavior and provide instant responses, instant gratification, and instant engagement, which can result in users' addiction to such applications (Hawi and Samaha, 2017).

The results of the present review showed that mobile applications can directly reach 27 data points about each individual user. Furthermore, if the user makes use of a mobile device with other applications, the information that can be obtained from that user can add value to advertising segmentation strategies; in this way, personal data get monetized.

Furthermore, as highlighted by our results, another concern related to user privacy is related to defining who has access to the data. As demonstrated by our review, the beneficiaries in this case are private companies supported or subsidized by governments in their public health protocols to promote public health in the time of the COVID-19 pandemic. Governments must make good use of the collected data and inform users of relevant aspect of the data collection process, such as further use of the data, frequency of use, and so on.

In addition, users should be aware that, if they accept the terms of use of the applications they install on connected devices and mobile phones, the identification of an individual user is legal; however, problems can arise when companies such as Cambridge Analytica identify users and their online footprint collectively so they could massively modify their decisions, this is just a possibility that could become a reality if the management of user's information is carry out wrongly. Therefore, this kind of actions must be monitored. Likewise, the user should understand the importance of his/her information as they create a trace when using mobile applications to monetarize pandemics symptoms.

We are in a new digital age when the response of the society and the privacy of its individuals must be of their own choice, and not a new imposed standard for the management of user information (Cabalquinto and Hutchins, 2020). Concepts such as 'surveillance capitalism' (Zuboff, 2019) must not gain strength or cause this new era of surveillance to become an opportunity for mass control, disinformation, and mismanagement of information (Bu et al., 2020).

In this context, there emerges the following question: Should companies not offer both a paid version of their applications that does not collect user data, and a free or freemium version, based on the profitability of studying, analyzing and selling customer data?

All in all, the development of technological solutions to curb the pandemic through tracking users' mobile devices should not become a new form of social inequality based on the use of digital technologies and devices.

6. Conclusions

In the present study, we applied the SLR methodology to identify available technologies to monitor users with symptoms of COVID-19 and other future diseases. The identified technologies were also analyzed based on their characteristics and classified with respect to their uses and types of information they collect. Particular emphasis was placed on understanding user privacy concerns and identifying the data that can be obtained from users via these applications.

The results of our analysis showed that there are a total of 13 technologies that can be used by private companies, public institutions, and governments to control the COVID-19 and future pandemics. These 13 technologies are based on obtaining data, mostly about the location of the terminals; however, when combined, some of these technologies can yield more detailed information and help predict user behavior.

The identified technologies were classified based on the following aspect of data and data management: (1) security; (2) destruction; (3) voluntary access; (4) time span; and (5) storage. In addition, in order to understand how these technologies can affect user privacy, we identified 25 data points that these technologies could have access to if installed through mobile applications.

Furthermore, in order to explore the role of privacy in the use of user data, we classified the ways in which massive data from users can be collected. The results of our analysis showed the following three major sources of information about users: (1) location-based social networks (LBSN); (2) location-based services (LBS); and (3) location-based mobile services (LBMS) (see Table 6 for their definitions).

In addition, from the point of view of surveillance and user privacy, we identified a total of 25 data points that can be tracked both with the technologies presented and by applications that users use daily to surf the Internet or while using their connected devices.

The finding outlined above allowed us to answer the research questions addressed in the present study. First, regarding RQ1 ("What technologies based on collecting information from users' mobile devices can be massively used to track COVID-19 or future pandemics?") it has been found that location, Bluetooth, GPS, External API based on track users, DP-3T, ID Network Location, Textual Analysis, Logbook systems, Meta data, Data Logging, Online Tracking, Third-party sources and Mobile Crowd-sending could be used as sources to track COVID-19 and other future diseases symptoms and infections. For each of these technologies, the safety and reliability characteristics have been shown and analyzed as well as linked to user's privacy. Furthermore, regarding RQ2 ("What privacy risks of mass surveillance actions are associated with each tracking technology in the current emergency situation?"), the main risks that the use of these technologies can derive in user's privacy has been shown and discussed linking to problems relative to mass surveillance, information management and society prediction movements.

6.1. Theoretical implications

The results of the present study have theoretical implications for future research. First, the technologies identified, and concepts defined in this study allow for the development of new studies focused on what is known as surveillance capitalism and massive data collection.

Second, our results showed that there is an urgent need to protect the privacy of users who use mobile applications with location technologies and other data collection factors in a responsible and correct manner. To this end, in-depth interviews with opinion leaders and policymakers must be carried out so that they can spread messages of trust. Researchers should start creating literature based on the use of these technologies, with a particular focus on tracking disease symptoms and the role of information science in this area.

Third, the identified technologies must be studied in depth by academics, as well as put to the test by engineers and information science experts to ensure that the collection of massive data with the aim of preventing COVID-19 infections does not violate user privacy and does not generate serious security problems.

Fourth, our results open a new avenue of research that would seek for the justification for the use of data-collection technologies based on global public health concerns. Finally, this review can also be used to identify those relevant studies developed based on data collection using mobile technologies.

6.2. Implications for the industry

Private software development companies, as well as public institutions, governments, and organizations such as the World Health Organization (WHO) or the United Nations (UN), can use the results of the present study to understand which technologies can technically be used to control the spread of the COVID-19 pandemic.

While the technologies identified in the present review have been introduced prior to the outbreak of the COVID-19 pandemic, they have recently been proposed for the global use with the purpose of massive tracking for public health reasons.

In addition, we also reviewed several studies that exposed vulnerabilities associated with the use of these technologies and data collection services. Users must be aware of privacy policies; therefore, non-profit organizations and other public institutions, as well as practitioners and private companies, must be aware that they are obliged to inform users that their data will be monitored, deleted, and anonymized after a period of time established in the terms of use of the applications when tracking COVID-19 using mobile devices.

Finally, all parties that are granted access to user data should meet all standards of user privacy protection and rule out the risk of the data being sold to third parties. The data must be anonymized, and users must ensure that their data will be used exclusively for public health reasons and notifications.

6.3. Limitations and future research

The present study has several limitations. The first limitation is related to the methodological process where search terms were used to find previously published studies about monitoring user information through mobile devices. The second limitations is related to the rapid advance of the COVID-19 pandemic: as the coronavirus pandemic progresses, available information about this virus and the required information about the symptoms expands, which requires a fast adaptation of concerned technologies.

Despite the limitations outlined above, the results of the present study are meaningful in that we identify available methodologies to counteract the COVID-19 pandemics and expose the vulnerability of users whose privacy can be violated due the use of such technologies. Further research that would carefully tackle these problematic issues is warranted. Furthermore, future research studies focused on the analysis of any type of data sources such as connected devices, smart cities developments, voice assistants, or smart clothes, among other technologies and initiatives, should be considered by researchers as these could be used as surveillance technologies to predict users' movements, actions and behaviors.

Author's Statement

Conceptualization: S.R.N, J.R.S and D.P.M; Formal analysis: D.P.M; Investigation: S.R.N, J.R.S; Methodology: S.R.N, J.R.S; Resources: S.R.N, J.R.S and D.P.M; Software: S.R.N; Supervision: D.P.M; Validation: J.R.S; Visualization: J.R.S; Roles/Writing - original draft: S.R.N, J.R.S; Writing - review & editing: S.R.N, J.R.S and D.P.M.

References

… & Ahmed, N., Michelin, R.A., Xue, W., Ruj, S., Malaney, R., Kanhere, S.S., Jha, S.K., 2020. A survey of covid-19 contact tracing apps. IEEE Access 8, 134577–134601. https://doi.org/10.1109/ACCESS.2020.3010226.

Allmendinger, R.W., Siron, C.R., Scott, C.P., 2017. Structural data collection with mobile devices: accuracy, redundancy, and best practices. J. Struct. Geol. 102, 98–112. https://doi.org/10.1016/j.jsg.2017.07.011.

Aloi, D.N., Alsliety, M., Akos, D.M., 2007. A Methodology for the evaluation of a GPS receiver performance in telematics applications. IEEE Trans. Instrum. Meas. 56 (1), 11–24. https://doi.org/10.1109/tim.2006.887190.

Ando, R., Shima, S., Takemura, T., 2016. Analysis of privacy and security affecting the intention of use in personal data collection in an IoT environment. IEICE Trans. Inf. Syst. (8), 1974–1981. https://doi.org/10.1587/transinf.2015ini0002. E99.D.

Arriagada, J., Gschwender, A., Munizaga, M.A., Trépanier, M., 2018. Modeling bus bunching using massive location and fare collection data. J. Intell. Transp. Syst. 23 (4), 332–344. https://doi.org/10.1080/15472450.2018.1494596.

Arya, V., Sethi, D., Paul, J., 2019. Does digital footprint act as a digital asset? – Enhancing brand experience through remarketing. Int. J. Inf. Manag. 49, 142–156. https://doi.org/10.1016/j.ijinfomgt.2019.03.013.

Balapour, A., Nikkhah, H.R., Sabherwal, R., 2020. Mobile application security: role of perceived privacy as the predictor of security perceptions. Int. J. Inf. Manag. 52, 102063 https://doi.org/10.1016/j.ijinfomgt.2019.102063.

Beigi, G., Liu, H., 2020. A survey on privacy in social media: identification, mitigation, and applications. ACM Trans. Data Sci. 1 (1), 1–38. https://doi.org/10.1145/3343038.

Bem, D.J., 1995. Writing a review article for psychological bulletin. Psychol. Bull. 118 (2), 172–177. https://doi.org/10.1037/0033-2909.118.2.172.

Ben-Gal, I., Weinstock, S., Singer, G., Bambos, N., 2019. Clustering users by their mobility behavioral patterns. ACM Trans. Knowl. Discov. Data 13 (4), 1–28. https://doi.org/10.1145/3322126.

Blair, R.A., Morse, B.S., Tsai, L.L., 2017. Public health and public trust: survey evidence from the Ebola Virus Disease epidemic in Liberia. Soc. Sci. Med. 172, 89–97. https://doi.org/10.1016/j.socscimed.2016.11.016.

Blazquez, D., Domenech, J., 2018. Big Data sources and methods for social and economic analyses. Technol. Forecast. Soc. Change 130, 99–113. https://doi.org/10.1016/j.techfore.2017.07.027.

Bresciani, S., Ferraris, A., Del Giudice, M., 2018. The management of organizational ambidexterity through alliances in a new context of analysis: internet of Things (IoT) smart city projects. Technol. Forecast. Soc. Change 136, 331–338. https://doi.org/10.1016/j.techfore.2017.03.002.

Brocke, J.V., Simons, A., Riemer, K., Niehaves, B., Plattfaut, R., Cleven, A., 2015. Standing on the shoulders of giants: challenges and recommendations of literature search in information systems research. Commun. Assoc. Inf. Syst. 37. https://doi.org/10.17705/1cais.03709.

Bu, F., Wang, N., Jiang, B., Liang, H., 2020. Privacy by Design" implementation: information system engineers' perspective. Int. J. Inf. Manag. 53, 102124 https://doi.org/10.1016/j.ijinfomgt.2020.102124.

Buchanan, T., Paine, C., Joinson, A.N., Reips, U.D., 2007. Development of measures of online privacy concern and protection for use on the Internet. Journal of the American society for information science and technology 58 (2), 157–165.

Cabalquinto, E., Hutchins, B., 2020. "'It should allow me to opt in or opt out": investigating smartphone use and the contending attitudes of commuters towards geolocation data collection. Telemat. Inform. 51, 101403 https://doi.org/10.1016/j.tele.2020.101403.

Can, Z., Demirbas, M., 2015. Smartphone-based data collection from wireless sensor networks in an urban environment. J. Netw. Comput. Appl. 58, 208–216. https://doi.org/10.1016/j.jnca.2015.08.013.

Cao, X., Cong, G., Jensen, C.S., 2010. Mining significant semantic locations from GPS data. Proc. VLDB Endow. 3 (1–2), 1009–1020. https://doi.org/10.14778/1920841.1920968.

Chadwick, A., Collister, S., 2014. Boundary-drawing power and the renewal of professional news organizations: the case of the guardian and the Edward Snowden NSA leak. Int. J. Commun. 8, 22, 1932–8036/20140005.

Chai, J., Nayak, T.K., 2018. A criterion for privacy protection in data collection and its attainment via randomized response procedures. Electron. J. Stat. 12 (2), 4264–4287. https://doi.org/10.1214/18-ejs1508.

Chakraborty, I., Maity, P., 2020. COVID-19 outbreak: migration, effects on society, global environment and prevention. Sci. Total Environ., 138882 https://doi.org/10.1016/j.scitotenv.2020.138882.

Chandra, B., Sudarshan, S., 2017. Runtime optimization of join location in parallel data management systems. Proc. VLDB Endow. 10 (11), 1490–1501. https://doi.org/10.14778/3137628.3137656.

Chen, L., Meservy, T.O., Gillenson, M., 2012. Understanding information systems continuance for information-oriented mobile applications. Commun. Assoc. Inf. Syst. 30. https://doi.org/10.17705/1cais.03009.

Cheng, X., Fang, L., Yang, L., 2018. Mobile big data based network intelligence. IEEE Internet Things J. 5 (6), 4365–4379.

Choi, J.P., Jeon, D.-.S., Kim, B.-.C., 2018. Privacy and personal data collection with information externalities. SSRN Electron. J. https://doi.org/10.2139/ssrn.3115049.

Craker, N., March, E., 2016. The dark side of Facebook®: the Dark Tetrad, negative social potency, and trolling behaviours. Pers. Individ. Dif. 102, 79–84. https://doi.org/10.1016/j.paid.2016.06.043.

Dimitriou, T., Krontiris, I., 2017. Privacy-respecting auctions and rewarding mechanisms in mobile crowd-sensing applications. J. Netw. Comput. Appl. 100, 24–34. https://doi.org/10.1016/j.jnca.2017.10.012.

Elia, G., Margherita, A., Passiante, G., 2020. Digital entrepreneurship ecosystem: how digital technologies and collective intelligence are reshaping the entrepreneurial process. Technol. Forecast. Soc. Change 150, 119791. https://doi.org/10.1016/j.techfore.2019.119791.

Fengzhe, Z., Jin, C., Haibo, C., Binyu, Z., 2011. Lifetime privacy and self-destruction of data in the cloud. J. Comput. Res. Dev. 7.

Gayness Clark, J, Lang Beebe, N, Williams, K, Shepherd, L, 2009. Security and privacy governance: criteria for systems design. J. Inf. Priv. Secur. 5 (4), 3–30. https://doi.org/10.1080/15536548.2009.10855873.

Gerke, S., Shachar, C., Chai, P.R., Cohen, I.G., 2020. Regulatory, safety, and privacy concerns of home monitoring technologies during COVID-19. Nat. Med. 26 (8), 1176–1182. https://doi.org/10.1038/s41591-020-0994-1.

Giroux, S.A., Kouper, I., Estes, L.D., Schumacher, J., Waldman, K., Greenshields, J.T., Evans, T.P., 2019. A high-frequency mobile phone data collection approach for research in social-environmental systems: applications in climate variability and food security in sub-Saharan Africa. Environ. Model. Softw. 119, 57–69. https://doi.org/10.1016/j.envsoft.2019.05.011.

Gogus, A., Saygın, Y., 2019. Privacy Perception and Information Technology Utilization of High School Students, 5. Heliyon. https://doi.org/10.1016/j.heliyon.2019.e01614.

Gonzalez-Loureiro, M., Dabić, M., Kiessling, T., 2015. Supply chain management as the key to a firm's strategy in the global marketplace. Int. J. Phys. Distrib. Logist. Manag. 45 (1/2), 159–181. https://doi.org/10.1108/IJPDLM-05-2013-0124.

Grover, J., 2013. Android forensics: automated data collection and reporting from a mobile device. Digit. Invest. 10. https://doi.org/10.1016/j.diin.2013.06.002.

Guo, A., Ma, J., 2017. Context-aware scheduling in personal data collection from multiple wearable devices. IEEE Access 5, 2602–2614. https://doi.org/10.1109/access.2017.2666419.

Guy, J.S., 2019. Digital technology, digital culture and the metric/nonmetric distinction. Technol. Forecast. Soc. Change 145, 55–61. https://doi.org/10.1016/j.techfore.2019.05.005.

Hawi, N.S., Samaha, M., 2017. The relations among social media addiction, self-esteem, and life satisfaction in university students. Soc. Sci. Comput. Rev. 35 (5), 576–586. https://doi.org/10.1177/0894439316660340.

Hermalin, B.E., Katz, M.L., 2006. Privacy, property rights and efficiency: the economics of privacy as secrecy. Quant. Mark. Econ. 4 (3), 209–239. https://doi.org/10.1007/s11129-005-9004-7.

Ho, S.-.C., Chen, J.-.L., Luo, S.-.T., 2015. What users want: the factors that determine the retention of social location-based services. Pac. Asia J. Assoc. Inf. Syst. 49–78. https://doi.org/10.17705/1pais.07103.

Hsieh, H.-.P., Li, C.-.T., Lin, S.-.D., 2014. Measuring and recommending time-sensitive routes from location-based data. ACM Trans. Intell. Syst. Technol. 5 (3), 1–27. https://doi.org/10.1145/2542668.

Hu, H., Xu, J., On, S.T., Du, J., Ng, J.K.Y, 2010. Privacy-aware location data publishing. ACM Trans. Database Syst. 35 (3), 1–42. https://doi.org/10.1145/1806907.1806910.

Irache, A., Murachpersad, R., Caleyachetty, R., 2019. The development and application of a mobile-based data collection system for a growth monitoring programme in selected primary care centres in the Republic of Mauritius. BMJ Global Health 4 (6), e001928. https://doi.org/10.1136/bmjgh-2019-001928.

Isaak, J., Hanna, M.J., 2018. User data privacy: Facebook, Cambridge Analytica, and privacy protection. Comput. Long Beach Calif. 51 (8), 56–59. https://doi.org/10.1109/MC.2018.3191268.

Ivanov, D., 2020. Predicting the impacts of epidemic outbreaks on global supply chains: a simulation-based analysis on the coronavirus outbreak (COVID-19/SARS-CoV-2) case. Transp. Res. E Logist. Transp. Rev. 136, 101922 https://doi.org/10.1016/j.tre.2020.101922.

Jensen, C., Potts, C., Jensen, C., 2005. Privacy practices of Internet users: self-reports versus observed behavior. Int. J. Hum. Comput. Stud. 63 (1–2), 203–227.

Jho, W., Song, K.J., 2015. Institutional and technological determinants of civil e-Participation: Solo or duet? Gov. Inform. Quart. 32 (4), 488–495.

Jin, H., Liu, M., Dodhia, K., Li, Y., Srivastava, G., Fredrikson, M., Hong, J.I, 2018. Why are they collecting my data? Proc. ACM Interact. Mobile Wear. Ubiq. Technol. 2 (4), 1–27. https://doi.org/10.1145/3287051.

Jin, Y., Liu, B.F., Austin, L.L., 2014. Examining the role of social media in effective crisis management: the effects of crisis origin, information form, and source on publics' crisis responses. Commun. Res. 41 (1), 74–94. https://doi.org/10.1177/0093650211423918.

Kaashoek, J., & Santillana, M. (2020). COVID-19 positive cases, evidence on the time evolution of the epidemic or an indicator of local testing capabilities? A case study in the United States. doi: 10.2139/ssrn.3574849.

Kaciak, E., Louviere, J., 1990. Multiple correspondence analysis of multiple choice experiment data. J. Mark. Res. 27 (4), 455–465. https://doi.org/10.1177/002224379002700407.

Kang, Y., Yang, K.C.C, 2020. What do Facebook users feel about Facebook advertising? Impacts of online advertising on business performance advances in marketing. Custom. Relat. Manag. E Serv. 1–27. https://doi.org/10.4018/978-1-7998-1618-8.ch001.

Karas, S., 2002. Enhancing the privacy discourse: consumer information gathering as surveillance. J. Tech. L. Pol'y 7, 29.

Kavota, J.K., Kamdjoug, J.R.K., Wamba, S.F, 2020. Social media and disaster management: case of the north and south Kivu regions in the Democratic Republic of the Congo. Int. J. Inf. Manag. 52, 102068 https://doi.org/10.1016/j.ijinfomgt.2020.102068.

Keith, M., Babb, J., Furner, C., Abdullat, A., Lowry, P., 2016. Limited information and quick decisions: consumer privacy calculus for mobile applications. AIS Trans. Hum. Comput. Interact. 8 (3), 88–130. https://doi.org/10.17705/1thci.00081.

Kelley, P.G., Consolvo, S., Cranor, L.F., Jung, J., Sadeh, N., Wetherall, D., 2012. A conundrum of permissions: installing applications on an android smartphone. International Conference on Financial Cryptography and Data Security. Springer, Berlin, Heidelberg, pp. 68–79.

Khan, F., Rehman, A.U., Zheng, J., Jan, M.A., Alam, M., 2019. Mobile crowdsensing: a survey on privacy-preservation, task management, assignment models, and incentives mechanisms. Future Gener. Comput. Syst. 100, 456–472. https://doi.org/10.1016/j.future.2019.02.014.

Kiessling, T., Vlačić, B., Dabić, M., 2019. Mapping the future of cross-border mergers and acquisitions: a review and research agenda. IEEE Trans. Eng. Manag. 99, 1–11. https://doi.org/10.1109/TEM.2019.2954799.

Kim, J.W., Jang, B., 2019. Workload-aware indoor positioning data collection via local differential privacy. IEEE Commun. Lett. 23 (8), 1352–1356. https://doi.org/10.1109/lcomm.2019.2922963.

Kim, R.Y., 2020. The impact of COVID-19 on consumers: preparing for digital sales. IEEE Eng. Manag. Rev. https://doi.org/10.1109/EMR.2020.2990115.

Knijnenburg, B.P., Kobsa, A., Jin, H., 2013. Preference-based location sharing: are more privacy options really better?. In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, pp. 2667–2676.

Koshimizu, T., Toriyama, T., Babaguchi, N., 2006. Factors on the sense of privacy in video surveillance. In: Proceedings of the 3rd ACM Workshop on Continuous Archival and Retrival of Personal Experences, pp. 35–44. https://doi.org/10.1145/1178657.1178665.

Kummitha, R.K.R, 2020. Smart technologies for fighting pandemics: the techno-and human-driven approaches in controlling the virus transmission. Gov. Inf. Q., 101481 https://doi.org/10.1016/j.giq.2020.101481.

LaBrie, R.C., Steinke, G.H., Li, X., Cazier, J.A., 2018. Big data analytics sentiment: uS-China reaction to data collection by business and government. Technol. Forecast. Soc. Change 130, 45–55. https://doi.org/10.1016/j.techfore.2017.06.029.

... & Lambrecht, A., Goldfarb, A., Bonatti, A., Ghose, A., Goldstein, D.G., Lewis, R., Yao, S., 2014. How do firms make money selling digital goods online?. Mark. Lett. 25 (3), 331–341. https://doi.org/10.1007/s11002-014-9310-5.

Langley, D.J., van Doorn, J., Ng, I.C., Stieglitz, S., Lazovik, A., Boonstra, A., 2020. The Internet of everything: smart things and their impact on business models. J. Bus. Res. https://doi.org/10.1016/j.jbusres.2019.12.035.

Lee, Y.-.L., Tsai, W.-.H., 2014. A new data hiding method via revision history records on collaborative writing platforms. ACM Trans. Multimed. Comput. Commun. Appl. 10 (2), 1–21. https://doi.org/10.1145/2534408.

Leite, H., Hodgkinson, I.R., Gruber, T., 2020. New development:'Healing at a distance'—telemedicine and COVID-19. Public Money Manag. 1–3. https://doi.org/10.1080/09540962.2020.1748855.

Lesani, A., Miranda-Moreno, L., 2019. Development and testing of a real-time WiFi-bluetooth system for pedestrian network monitoring, classification, and data extrapolation. IEEE Trans. Intell. Transp. Syst. 20 (4), 1484–1496. https://doi.org/10.1109/tits.2018.2854895.

Li, H., Ma, J., Fu, S., 2015. A privacy-preserving data collection model for digital community. Sci. China Inf. Sci. 58 (3), 1–16. https://doi.org/10.1007/s11432-014-5197-2.

Libaque-Sáenz, C.F., Wong, S.F., Chang, Y., Bravo, E.R., 2020. The effect of fair information practices and data collection methods on privacy-related behaviors: a study of Mobile apps. Inf. Manag., 103284 https://doi.org/10.1016/j.im.2020.103284.

Liu, S., Du, J., Shrivastava, A., Zhong, L., 2019. Privacy adversarial network. In: Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies, 3, pp. 1–18. https://doi.org/10.1145/3369816.

Luceri, L., Cardoso, F., Papandrea, M., Giordano, S., Buwaya, J., Kundig, S., Mitrokotsa, A., 2018. VIVO: a secure, privacy-preserving, and real-time crowd-sensing framework for the Internet of Things. Pervasive Mob. Comput. 49, 126–138. https://doi.org/10.1016/j.pmcj.2018.07.003.

Malhotra, N.K., Kim, S.S., Agarwal, J., 2004. Internet users' information privacy concerns (IUIPC): the construct, the scale, and a causal model. Inf. Syst. Res. 15 (4), 336–355. https://doi.org/10.1287/isre.1040.0032.

Mantelero, A., 2013. The EU proposal for a general data protection regulation and the roots of the 'right to be forgotten. Comput. Law Secur. Rev. 29 (3), 229–235. https://doi.org/10.1016/j.clsr.2013.03.010.

Mckenzie, G., Slind, R.T., 2019. A user-generated data based approach to enhancing location prediction of financial services in sub-Saharan Africa. Appl. Geogr. 105, 25–36. https://doi.org/10.1016/j.apgeog.2019.02.005.

Mennecke, B.E., West Jr, L.A, 2001. Geographic Information Systems in developing countries: issues in data collection, implementation and management. J. Global Inf. Manag. 9 (4), 44–54.

Moher, D., Liberati, A., Tetzlaff, J., Altman, D.G., The PRISMA Group, 2009. Preferred reporting items for systematic reviews and MetaAnalyses: The PRISMA statement. PLoS Med. 6 (7), e1000097. https://doi.org/10.1371/journal.pmed1000097.

Mokbel, M., Chow, C.-.Y., Aref, W., 2016. Location data management. Proc. VLDB Endow. 9 (13) https://doi.org/10.14778/3007263.3007327, 1622–1622.

Moore, A.D., 2011. Privacy, security, and government surveillance: wikileaks and the new accountability. Public Aff. Q. 25 (2), 141–156.

Mulvenna, M.D., Anand, S.S., Büchner, A.G., 2000. Personalization on the Net using Web mining: introduction. Commun. ACM 43 (8), 122–125. https://doi.org/10.1145/345124.345165.

Mun, M.Y., Kim, D.H., Shilton, K., Estrin, D., Hansen, M., Govindan, R., 2014. PDVLoc. ACM Trans. Sens. Netw. 10 (4), 1–29. https://doi.org/10.1145/2523820.

Nguyen, M.T., 2020. Distributed compressive and collaborative sensing data collection in mobile sensor networks. Internet Things 9, 100156. https://doi.org/10.1016/j.iot.2019.100156.

Paine, C., Reips, U.D., Stieger, S., Joinson, A., Buchanan, T., 2007a. Internet users' perceptions of 'privacy concerns' and 'privacy actions. Int. J. Hum. Comput. Stud. 65 (6), 526–536. https://doi.org/10.1016/j.ijhcs.2006.12.001.

Palos-Sanchez, P., Saura, J.R., Martin-Velicia, F., 2019. A study of the effects of programmatic advertising on users concerns about privacy overtime. J. Bus. Res. 96, 61–72. https://doi.org/10.1016/j.jbusres.2018.10.059.

Pan, S.L., Cui, M., Qian, J., 2020. Information resource orchestration during the COVID-19 pandemic: a study of community lockdowns in China. Int. J. Inf. Manag. 54, 102143 https://doi.org/10.1016/j.ijinfomgt.2020.102143.

Perentis, C., Vescovi, M., Leonardi, C., Moiso, C., Musolesi, M., Pianesi, F., Lepri, B., 2017. Anonymous or not? Understanding the factors affecting personal mobile data disclosure. ACM Trans. Internet Technol. 17 (2), 1–19. https://doi.org/10.1145/3017431.

Qi, J., Yang, P., Newcombe, L., Peng, X., Yang, Y., Zhao, Z., 2020. An overview of data fusion techniques for Internet of Things enabled physical activity recognition and measure. Inf. Fus. 55, 269–280. https://doi.org/10.1016/j.inffus.2019.09.002.

Rashidi, Y., Vaniea, K., 2015. Poster: a user study of Whatsapp privacy settings among Arab users. In: Proceedings of the IEEE Symposium on Security and Privacy.

Reyes-Menendez, A., Saura, J.R., Stephen, B.T., 2019. Exploring key indicators of social identity in the #MeToo era: using discourse analysis in UGC. Int. J. Inf. Manag. 54, 102129 https://doi.org/10.1016/j.ijinfomgt.2020.102129.

Sajjad, H., Kanwal, T., Anjum, A., Malik, S.U.R., Khan, A., Khan, A., Manzoor, U, 2019. An efficient privacy preserving protocol for dynamic continuous data collection. Comput. Secur. 86, 358–371. https://doi.org/10.1016/j.cose.2019.06.017.

Salo, M., Makkonen, M., 2018. Why do users switch mobile applications? Trialing behavior as a predecessor of switching behavior. Commun. Assoc. Inf. Syst. 42, 386–407. https://doi.org/10.17705/1cais.04214.

Sang, J., Fang, Q., Xu, C., 2017. Exploiting social-mobile information for location visualization. ACM Trans. Intell. Syst. Technol. 8 (3), 1–19. https://doi.org/10.1145/3001594.

Saura, J.R., 2020. Using data sciences in digital marketing: framework, methods, and performance metrics. J. Innov. Knowl. 1 https://doi.org/10.1016/j.jik.2020.08.001, 2020.

Saura, J.R., Rodriguez Herráez, B, Reyes-Menendez, A., 2019. Comparing a traditional approach for financial brand communication analysis with a big data analytics technique. IEEE Access 7 (1). https://doi.org/10.1109/ACCESS.2019.2905301.

Saura, J.R., Ribeiro, D., Palacios-Marqués, E.R., 2021. From user-generated data to data-driven innovation: A research agenda to understand user privacy in digital markets. International Journal of Information Management. https://doi.org/10.1016/j.ijinfomgt.2021.102331. In Press.

Schobel, J., Probst, T., Reichert, M., Schlee, W., Schickler, M., Kestler, H., Pryss, R., 2020. Measuring mental effort for creating mobile data collection applications. Int. J. Environ. Res. Public Health 17 (5), 1649. https://doi.org/10.3390/ijerph17051649.

Scuotto, V., Ferraris, A., Bresciani, S., Al-Mashari, M., Del Giudice, M., 2016. Internet of Things: applications and challenges in smart cities. A case study of IBM smart city projects. Bus. Process Manag. J. https://doi.org/10.1108/BPMJ-05-2015-0074.

Shafer, S.M., Smith, H.J., Linder, J.C., 2005. The power of business models. Bus. Horiz. 48 (3), 199–207. https://doi.org/10.1016/j.bushor.2004.10.014.

Shilton, K., 2009. Four billion little brothers? Privacy, mobile phones, and ubiquitous data collection. Commun. ACM 52 (11), 48–53. https://doi.org/10.1145/1592761.1592778.

Silva, T.H., Viana, A.C., Benevenuto, F., Villas, L., Salles, J., Loureiro, A., Quercia, D., 2019. Urban computing leveraging location-based social network data. ACM Comput. Surv. 52 (1), 1–39. https://doi.org/10.1145/3301284.

Sinha, G.A., 2013. NSA surveillance since 9/11 and the human right to privacy. Loy. L. Rev. 59, 861.

Spolaor, R., Santo, E.D., Conti, M., 2017. DELTA: data extraction and logging tool for android. IEEE Trans. Mobile Comput. 17 (6), 1289–1302. https://doi.org/10.1109/tmc.2017.2762692.

Stamoulis, D., Gouscos, D., Georgiadis, P., Martakos, D., 2001. Revisiting public information management for effective e-government services. Inf. Manag. Comput. Secur. https://doi.org/10.1108/09685220110400327.

Steenbruggen, J., Tranos, E., Nijkamp, P., 2015. Data from mobile phone operators: a tool for smarter cities? Telecomm. Policy 39 (3–4), 335–346. https://doi.org/10.1016/j.telpol.2014.04.001.

Steinfeld, N., 2016. I agree to the terms and conditions": (how) do users read privacy policies online? An eye-tracking experiment. Comput. Hum. Behav. 55, 992–1000. https://doi.org/10.1016/j.chb.2015.09.038.

Stieglitz, S., Mirbabaie, M., Ross, B., Neuberger, C., 2018. Social media analytics – challenges in topic discovery, data collection, and data preparation. Int. J. Inf. Manag. 39, 156–168. https://doi.org/10.1016/j.ijinfomgt.2017.12.002.

Stills, J.D., Hicks, J.M., Cain, A.A., 2020. Examining the influence of saliency in mobile interface displays. AIS Trans. Hum. Comput. Interact. 28–44. https://doi.org/10.17705/1thci.00127.

Suganya, M.S., 2018. Preventing the data over-collection in smart city via secure protection. Int. J. Res. Appl. Sci. Eng. Technol. 6 (4), 1945–1949. https://doi.org/10.22214/ijraset.2018.4333.

Svantesson, D.J.B, 2015. The (uncertain) future of online data privacy. Masaryk UJL Tech 9, 129.

Tan, K.H., Zhan, Y., 2017. Improving new product development using big data: a case study of an electronics company. R&D Manag. 47 (4), 570–582. https://doi.org/10.1111/radm.12242.

Taylor, I., 2017. Data collection, counterterrorism and the right to privacy. Polit. Philos. Econ. 16 (3), 326–346. https://doi.org/10.1177/1470594x17715249.

Terlizzi, M., Brandimarte, L., Sanchez, O., 2019. Replication of Internet privacy concerns in the mobile banking context. AIS Trans. Replic. Res. 5, 1–18. https://doi.org/10.17705/1atrr.00040.

Tuunanen, T., Peffers, K., Gengler, C.E., Hui, W., Virtanen, V., 2006. Developing feature sets for geographically diverse external end users: a call for value-based preference modeling. J. Inf. Technol. Theory Appl. 8 (2), 5.

Vankipuram, A., Vankipuram, M., Ghaemmaghami, V., Patel, V.L., 2017. A mobile application to support collection and analytics of real-time critical care data. Comput. Methods Programs Biomed. 151, 45–55. https://doi.org/10.1016/j.cmpb.2017.08.014.

Vargo, C.J., Hopp, T., 2020. Fear, anger, and political advertisement engagement: a computational case study of Russian-linked Facebook and Instagram content. J. Mass Commun. Q., 107769902091188 https://doi.org/10.1177/1077699020911884.

Venturini, T., Rogers, R., 2019. API-based research" or how can digital sociology and journalism studies learn from the Facebook and Cambridge analytica data breach. Digit. Journal. 7 (4), 532–540. https://doi.org/10.1080/21670811.2019.1591927.

vom Brocke, J., Simons, A., Niehaves, B., Riemer, K., Plattfaut, R., Cleven, A., 2009. Reconstructing the giant: on the importance of rigour in documenting the literature search process. In: ECIS 2009 Proceedings.

Wang, A., Shen, J., Wang, C., Yang, H., Liu, D., 2019. Anonymous data collection scheme for cloud-aided mobile edge networks. Digit. Commun. Netw. https://doi.org/10.1016/j.dcan.2019.04.001.

Wang, C.J., Ng, C.Y., Brook, R.H., 2020. Response to COVID-19 in Taiwan: big data analytics, new technology, and proactive testing. JAMA 323 (14), 1341–1342. https://doi.org/10.1001/jama.2020.3151.

Wang, K., Mi, J., Xu, C., Zhu, Q., Shu, L., Deng, D.J., 2016. Real-time load reduction in multimedia big data for mobile Internet. ACM Trans. Multimed. Comput. Commun. Appl. 12, 1–20. https://doi.org/10.1145/2990473 (5s).

Wang, W., Zhang, Q., 2016. Privacy preservation for context sensing on smartphone. IEEE ACM Trans. Netw. 24 (6), 3235–3247. https://doi.org/10.1109/tnet.2015.2512301.

Wang, X., Wang, L., Li, Y., Gai, K., 2018. Privacy-aware efficient fine-grained data access control in Internet of medical things based fog computing. IEEE Access 6, 47657–47665. https://doi.org/10.1109/access.2018.2856896.

Webster, J., Watson, R.T., 2002. Analyzing the past to prepare for the future: Writing a literature review. MIS Quarterly 26 (2), xiii–xxiii.

Wen, H., Zhao, Q., Lin, Z., Xuan, D., Shroff, N., 2020. A study of the privacy of covid-19 contact tracing apps. In: Proceedings of the International Conference on Security and Privacy in Communication Systems. Springer, Cham, pp. 297–317.

Wilson, E.V., Djamasbi, S., 2019. Measuring mobile user experience instruments for research and practice. Commun. Assoc. Inf. Syst. 44, 168–182. https://doi.org/10.17705/1cais.04408.

Wu, Y., Minkus, T., Ross, K.W., 2017. Taking the Pulse of US college campuses with location-based anonymous mobile apps. ACM Trans. Intell. Syst. Technol. 9 (1), 1–18. https://doi.org/10.1145/3078843.

Xu, L., Jiang, C., Chen, Y., Ren, Y., Liu, K.J.R, 2015. Privacy or utility in data collection? A contract theoretic approach. IEEE J. Sel. Top. Signal Process. 9 (7), 1256–1269. https://doi.org/10.1109/jstsp.2015.2425798.

Xu, X., Hu, H., Ha, S., Han, D., 2016. Smartphone-assisted spatial data collection improves geographic information quality: pilot study using a birth records dataset. Geospat. Health 11 (3). https://doi.org/10.4081/gh.2016.482.

Yao, G., Bi, J., Vasilakos, A.V., 2015. Passive IP Traceback: disclosing the locations of IP Spoofers from path backscatter. IEEE Trans. Inf. Foren. Secur. 10 (3), 471–484. https://doi.org/10.1109/tifs.2014.2381873.

Yaqub, U., Sharma, N., Pabreja, R., Chun, S.A., Atluri, V., Vaidya, J., 2020. Location-based sentiment analyses and visualization of Twitter election data. Digit. Gov. Res. Pract. 1 (2), 1–19. https://doi.org/10.1145/3339909.

Yu, Z., Tian, M., Wang, Z., Guo, B., Mei, T., 2016. Shop-type recommendation leveraging the data from social media and location-based services. ACM Trans. Knowl. Discov. Data 11 (1), 1–21. https://doi.org/10.1145/2930671.

Zhang, B., Liu, C.H., Lu, J., Song, Z., Ren, Z., Ma, J., Wang, W., 2016. Privacy-preserving QoI-aware participant coordination for mobile crowdsourcing. Comput. Netw. 101, 29–41. https://doi.org/10.1016/j.comnet.2015.12.022.

Zhang, D., Adipat, B., Mowafi, Y., 2009. User-centered context-aware mobile applications–the next generation of personal mobile computing. Commun. Assoc. Inf. Syst. 24. https://doi.org/10.17705/1cais.02403.

Zhang, W., Wang, M., Zhu, Y.-.C., 2020. Does government information release really matter in regulating contagion-evolution of negative emotion during public emergencies? From the perspective of cognitive big data analytics. Int. J. Inf. Manag. 50, 498–514. https://doi.org/10.1016/j.ijinfomgt.2019.04.001.

Zhou, T., Cai, Z., Xiao, B., Wang, L., Xu, M., Chen, Y., 2018. Location privacy-preserving data recovery for mobile crowdsensing. In: Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies, 2, pp. 1–23.

Zhu, W.-.Y., Peng, W.-.C., Chen, L.-.J., Zheng, K., Zhou, X., 2016. Exploiting viral marketing for location promotion in location-based social networks. ACM Trans. Knowl. Discov. Data 11 (2), 1–28. https://doi.org/10.1145/3001938.

Zuboff, S., 2015. Big other: surveillance capitalism and the prospects of an information civilization. J. Inf. Technol. 30 (1), 75–89. https://doi.org/10.1057/jit.2015.5.

Zuboff, S., 2019. The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. Profile Books.

Samuel Ribeiro-Navarrete Graduated in Finance and Accounting with a Master's degree in digital business and finance, Samuel has contributed to numerous national and international research congresses with papers and conferences related to his field of specialization. Samuel's research is focused on the study of international business, finance and accounting, as well as its connection to technology. He has contributed as a reviewer and author to numerous Research Journals.

Jose Ramon Saura is Researcher and Associate professor of Digital Marketing in the Business Economics Department at Rey Juan Carlos University, Madrid (Spain). Previously, he held positions and made consultancy at a number of other companies including Google, L'Oreal, Deloitte, Telefónica, or MRM//McCann, among others. He earned an international Ph.D. in Digital Marketing at the Rey Juan Carlos University, while researching at London South Bank University (LSBU) and Harvard University (RCC at Harvard).His research has focused on the theoretical and practical insights of various aspects of User Generated Data and Content (UGD - UGC), with a specific focus around three major research approaches applied to business and marketing: data mining, knowledge discovery, and information sciences. His research has appeared in leading business, marketing and information sciences journals such as: Journal of Innovation and Knowledge, International Journal of Information Management, Journal of Business Research, Review of Managerial Sciences, Journal of Business & Industrial Marketing, IEEE Access, among others.

Daniel is Director of the Master in Direction and Management of Digital Businesses in Universitat Politècnica de València. Daniel has published in Journal such as Tourism Management, Annals of Tourism Research, Small Business Economics, Management Decision, International Journal of Technology Management, Cornell Quarterly Management, Services Industries Journal, Service Business, International Entrepreneurship and Management Journal, Journal of Knowledge Management, Journal of Intellectual Capital, International Journal of Sport Policy and Politics, International Journal of Computational Intelligence Systems, International Journal of Innovation Management and International Journal of Contemporary Hospitality Management, Kybernetes, Human Resource Management, International Journal of Project Management, Technological and Economic Development of Economy, Journal of Organizational Change Management. He is currently Associate Editor of Personnel Review Journal. He has been the winner of the 1st Research Prize at the II Convocatòria de Premis de Prospectiva de l'Agència Valenciana d'Avaluació i Acreditació.