Privacy during Pandemic: A Global View of Privacy Practices around COVID-19 Apps

Tanusree Sharma
tsharma6@illinois.edu
University of Illinois at Urbana-Champaign
Champaign, USA

Md Mirajul Islam
mislam22@ncsu.edu
North Carolina State University
Raleigh, USA

Anupam Das
anupam.das@ncsu.edu
North Carolina State University
North Carolina, USA

S. M. Taiabul Haque
haque@ucmo.edu
University of Central Missouri
Warrensburg, USA

Syed Ishtiaque Ahmed
ishtiaque@cs.toronto.edu
University of Toronto
Ontario, USA

ABSTRACT

A large number of mobile phone applications have been built and deployed to combat COVID-19, offering various services to users, including virus information, contact tracing, and symptom monitoring among others. At the same time, the privacy and security vulnerabilities of user data over these apps have become a big concern in many places. To examine this issue, we conducted a mixed-method study with a combined approach of app analysis and an online survey to understand the privacy vulnerabilities of such apps and get an overview of user perceptions around this issue. In addition, we considered the notion of privacy in two different socio-economic contexts (Global North and Global South) to specify similarities and differences in app-specific privacy functionalities (data practices, functional requirements, regulations, etc.) and identify factors that impacted users' decision to use such apps (such as trust, preferences, concerns, motivations, etc.). Thus, this paper presents two diverse sets of opinions from these two geographic regions (including 27 countries), which provide a broader understanding of how the privacy concerns around COVID-19 are connected to various economic, political, and social factors. Furthermore, our analysis of 39 apps provides a deep insight into what many COVID-19 apps are lacking to ensure proper privacy practices and how those issues are entangled with various contextual challenges.

CCS CONCEPTS

• **Security and privacy → Privacy protections**.

KEYWORDS

COVID-19 Apps; static code analysis; privacy regulations

COMPASS '21, June 28-July 2, 2021, Virtual Event, Australia

ACM ISBN 978-1-4503-8453-7/21/06…$15.00
https://doi.org/10.1145/3460112.3471958

ACM Reference Format:
Tanusree Sharma, Md Mirajul Islam, Anupam Das, S. M. Taiabul Haque, and Syed Ishtiaque Ahmed. 2021. Privacy during Pandemic: A Global View of Privacy Practices around COVID-19 Apps. In *ACM SIGCAS Conference on Computing and Sustainable Societies (COMPASS) (COMPASS '21), June 28-July 2, 2021, Virtual Event, Australia.* ACM, New York, NY, USA, 15 pages. https://doi.org/10.1145/3460112.3471958

1 INTRODUCTION

Medical experts and scientists all over the world have been relying on mobile apps to educate and provide real-time information regarding the spread of COVID-19 (popularly known as coronavirus). These mobile apps are offering a wide variety of services, ranging from symptom checking to contact tracing, and from health monitoring to location-based awareness [46]. While different regions around the world have adopted these technologies differently based on their digital infrastructure, cultural norms, and political structure [56], it is imperative that we also critically examine the privacy and security guarantees they provide.

The burgeoning technology-led solutions to contain/control the pandemic raises many important ethical issues, including those of user privacy. For example, mobile apps that are designed to limit coronavirus exposure usually request different private and sensitive information from users, and access to certain permissions on their phones to operate effectively. When these apps are collecting and processing users' information, there is a huge potential for privacy and security risks when appropriate measures are not in place. It might be possible for apps to collect certain information without the user's knowledge or consent [38]. It may also be possible that a user does not knowingly share information including photos, contacts, location, and other private information [38]. Furthermore, lack of data protection laws/practices in certain regions may expose users to additional vulnerabilities [38]. To implement proper privacy mechanisms and design controls that focus on empowering people to protect their privacy, a comprehensive analysis is needed for the current global landscape of COVID-19 mitigation apps. Although there are few works that have examined security and privacy features such as cryptographic preservation, implementation of secure Bluetooth technology, or permission list of COVID-19 apps [22, 46, 55], to the best of our knowledge, there has not been any comprehensive global study that examines the privacy

regulations imposed by the local governments and the perceptions of the local users about COVID-19 apps.

Our paper aims to fill this gap in the existing HCI literature on COVID-19 apps. In this paper, we focus on analyzing the privacy risks that result from the absence of regulatory frameworks and compliance, and lack of user awareness in the host region. To this end, we first select a sample of 39 COVID-19 apps from 39 different countries, covering six continents. Next, we conduct a manual analysis of these apps with respect to the local regulatory frameworks and compliance laws on privacy. We follow up with a global user survey of 261 participants from 27 different countries, where we try to understand users' motivations, perceptions, privacy concerns, privacy preferences, and trust and transparency issues regarding COVID-19 apps.

Our findings highlight a clear division between the Global North and the Global South, in terms of both regulatory laws and user perceptions. In comparison to the Global South, the Global North apps tend to be more compliant with regulations, have more transparent privacy policy statements, and maintain relatively better data collection and retention practices. Our analysis of survey responses also reveals that the users from the Global North seem to be more reluctant to share personal information and location data whereas the Global South users are comfortable sharing those for contact tracing purposes, even with large corporations such as Apple and Google. However, regarding the motivation of using the apps and trusting non-profit organizations, the responses from both groups were more similar.

Taken together, our work provides a global perspective of privacy practices around COVID-19 apps and highlights the areas where the policymakers from the Global South need to work on to better protect user privacy. This paper thus contributes to a growing body of literature on the computer privacy and security challenges in the Global South [12–16, 18, 40, 41, 51]. The recent COVID-19 pandemic has made a significant impact on achieving Goal 3 (i.e., Good Health and Well-Being) of United Nations Sustainable Development Goals (SDGs) [9, 10], and we argue that without considering the privacy implications of COVID-19 apps in the context of local cultural norms and regulatory infrastructures, it is not possible to design sustainable solutions for improving the health and well-being of the general population.

The rest of the paper is organized as follows. Section 2 provides relevant background and highlights the related works. Section 3 describes our data collection and analysis methodology. We present our app analysis results and user survey responses in Section 4 and Section 5, respectively. Finally, we discuss the implications of our findings in Section 6.

2 BACKGROUND AND RELATED WORK

2.1 Privacy Perceptions and Risk Analysis of COVID-19 Apps

An increasing number of COVID-19 apps are being developed and released with the goal of tracking and reducing the spread of COVID-19. There are a large number of considerations that may influence user's willingness to install and use these apps. A person may weigh the features and the benefits of the app, the affiliation of the app provider, how well the app would preserve privacy [53], and the app's accuracy [55]. Understanding the impact of each of these factors can help app developers make design decisions that can maximize the impact. For understanding individual's privacy concerns and adoption of contact tracing mobile applications during a pandemic, researchers also seek to develop and empirically validate an integrative situational privacy calculus model for explaining potential privacy concerns and intention to install a contact tracing mobile application [42]. An individual's intention in this study is influenced by their risk beliefs, perceived individual and societal benefits to public health, privacy concerns, privacy protection initiatives, and technology features available. Studies also point out stigma and misconceptions over what government-proposed COVID-19 apps would entail [58]. Another study shows that the main factor that may facilitate or hinder the uptake is the trust (or lack of trust) in the government [20].

Prior studies have shown the prevalence of privacy and security threats for smartphones [28], including application development process around ready to use code into production without caution and expertise [35], poor authentication, authorization and session management [43], and lack of proper encryption of sensitive data [44]. Risk around user privacy is not much different during the period of coronavirus pandemic when companies, university research groups, and governments have been rapidly developing contact tracing apps to track and mitigate the spread of the virus. Existing research on COVID-19 apps analysis presents descriptive results and distribution of apps having different types of permission [22], how data is transported to the analytics center from users' devices [11], and what measures these apps have taken to ensure the privacy and security of users [39]. Furthermore, there are works that evaluate the comprehensibility of privacy policies of COVID-19 apps [60].

There are some recent studies on COVID-19 apps that recommend international strategies for regulation, evaluation, and use of digital technologies to strengthen pandemic management and future preparedness for pandemic [25] by addressing the challenges of implementing context-specific technology frameworks [57]. By considering cross-sectional issues, ethical and privacy concerns, studies also suggest process-based risk assessment and governance frameworks to guide different technological platforms and various phases in development of public health technology [36].

2.2 Design Space of COVID-19 apps

The most contentious issue that the current COVID-19 apps are facing is the deployment architecture (centralized vs. decentralized) as well as the corresponding technologies that underpin their functionality, including GPS, QR code, and Bluetooth that lead to privacy vulnerabilities [46]. In the centralized architecture, personal data collected through the app is controlled by government authority and it generally follows the Pan-European Privacy-Preserving Proximity Tracing (PEPP-PT) [30] protocol. However, the technical community considers this framework too pedantic for practical development [57]. For a decentralized approach, personal data are controlled by individuals only on personal devices and available apps generally follow the Decentralized Privacy-Preserving Proximity Tracing (DP-3T) [55] data protection solutions. However, this framework is only partially decentralized as there is an anonymous

centralized database for only the infected people. Google and Apple – in a joint partnership [50] – also launched an exclusive decentralized framework, which claims to be more compatible with Android and iOS systems, respectively. Technologies and infrastructures that underpin these two architectures are mainly based on GPS, QR code, and Bluetooth. GPS operates through crowd mapping for tracking the spread of COVID-19 while the QR code scanning approach is combined with physical temperature testing equipment or thermal imaging cameras to track the healthy or infected individuals' movement. The Bluetooth method detects other devices in proximity for a certain amount of time within a certain range of distance and notifies people who were in close proximity of an infected individual's device.

With these advanced technologies, there is a trade-off between data privacy and insights to make better decisions on mitigating COVID-19. Arguably, a decentralized and Bluetooth-based solution provides the highest level of data protection for individuals because no personal data is collected unless the individual is infected [46]. However, apps cannot collect and trace the movement of the population geographically without GPS tracking. Additionally, with a decentralized framework, any data collected from individuals cannot be exported into a centralized database for future analysis, which means less information would be processed for mandating self-quarantine and mitigating the spread of the disease, which can be a disadvantage for combating COVID-19. Secondly, existing decentralized COVID-19 apps such as Austria's Stopp Corona, STOP COVID-19 CAT, and SOS CORONA are issuing a static unique digital ID to each user with rolling public and private keys for message encryption and better data protection standard. If the digital ID is unique and static, it can cause risk if those IDs are hacked and paired with a mobile device, thus compromising individual privacy [57].

A few studies have been conducted based on the possible risk around COVID-19 contact tracing technology to build a protocol that ensures the protection of user privacy. There is a zero-knowledge protocol where no user can send fake messages to the system to launch a false positive attack [48]. Some of the recent proposed or implemented designs include implementation of decentralized proximity tracing [55], mechanisms with the construction of token in Bluetooth contact tracing [29], distributed hash table to build a decentralized messaging system for infected patients and their contacts [24], and blind signature to ensure that messages about infections are authentic and unchanged [24]. Privacy-preserving contact tracing apps are being proposed as well [28].

2.3 Impact of Privacy Regulations

There exist different regulatory approaches around the world to preserve users' privacy and security. For example, in the United States, the Privacy Act of 1974 establishes fair information practices to govern how individual's information is collected, maintained, used, and disseminated by federal agencies [8]. National Institute of Standards and Technology (NIST) developed a Privacy Framework which aims to improve privacy through optimized use of personal data [45]. Outside the US, different levels of international privacy laws and standards are being implemented in different regions. The APEC Privacy Framework was created for companies to demonstrate compliance with data privacy protection measures for members in the Asia-Pacific region [1]. European Union (EU) set up a universal privacy protection standard, which requires all Member States of the EU to transpose the directives in their national privacy laws [6]. Besides all these standards and guidelines, there are local privacy regulations in place to provide users with a certain level of data protection [23].

While there is considerable public discussion ongoing regarding coronavirus apps and the privacy of individuals, understanding the vulnerabilities of these apps can be an effective way to guide developers and policymakers. The majority of current studies addresses the privacy challenges and recommends the need for new forms of responsible and sustainable personal data governance model to implement ethical and regulatory principles [19], which can potentially increase the confidence of individuals and the society as a whole in personal data governance [37]. Some studies address the complexity and challenges of data practices in COVID-19 apps considering institutional, legal, cultural, and social factors [34] that need further comparative analysis to make concrete recommendations regarding regulatory frameworks. In general, studies suggest that regulatory guidelines focusing on pandemics can improve and protect the integrity of public data collection and processing mechanisms to maintain users' trust and eradicate their suspicions [59].

3 DATA COLLECTION AND METHODOLOGY

In this section, we discuss our research method for app collection, sampling, and assessment strategy.

App Collection and Sampling. In order to identify potential COVID-19 apps, we utilized a variety of keywords such as "COVID-19 app", "coronavirus app", "COVID-19 tracking", "COVID-19 contact tracing" to find relevant apps on the Google Play store. The full list of keywords used can be found in Appendix A. During our collection timeline (March 15, 2020 to April 30, 2020), we ended up with 97 COVID-19 apps. All of our collected apps were from the Android platform. The reason we focused on the Android platform was because of the availability of APK files, which were publicly accessible or obtainable from other websites unlike iOS. The collected apps mainly covered four different functionalities: contact tracing, self assessment, recent updates, and research data collection.

Our initial sample consisted of 97 COVID-19 Android apps designed for users from different parts of the world. For a deeper inspection, we filtered these apps based on the following two criteria: 1) one app from each country with the highest download count, which yielded apps from 48 different countries; 2) apps for which APK files were publicly available, which resulted in 39 apps in total (we were not able to download APK files for the remaining 9 apps). The full list of apps analyzed in this paper is available in Table 3 in Appendix B. Our selected 39 apps can be categorized into different groups based on ownership and functionalities they perform. Figure 1 shows the distribution of apps based on ownership, i.e., whether the app is provided by the state or a private sector company. Furthermore, in Figure 2, apps are divided into four categories based on the functionalities they provide such as recent updates/information, contact tracing, health assessment or research. In our selected apps, overall 27 out of 39 apps are for

tracking (e.g., contact tracing) purposes and it can also be seen that this type of apps is dominant across different regions.

App Assessment Methodology. In this section, we provide an overview of our assessment strategy for evaluating the privacy mechanisms implemented in the 39 collected COVID-19 apps.

Our evaluation process consists of the following steps:

(1) First, we carefully read each app's description page and if required, navigated to the corresponding websites and the privacy policy to gather the following information: [1] i) functionality; ii) protection mechanisms, iii) permission details, iv) data type collected, v) data-sharing practices, vi) data retention policy, vii) data processing policy, viii) regulatory compliance, ix) availability of privacy policy, x) opt-in/out control, xi) functional technology for data exchange (Bluetooth/GPS/Bluetooth+GPS), and xii) data storage architecture (centralization/decentralization). From this evaluation, our objective is to find out privacy criteria/benchmarks that are applied and gaps that might lead to potential privacy risks.

(2) While assessing the severity and sensitivity of different privacy and security measures of these 39 apps, we also contrast our findings across two regions: Global South and North.

User Survey. To assess users' attitudes toward using digital tracing apps and COVID-19 apps and the factors that might contribute to either positive or negative attitudes towards these technologies, we launch a user study consisting of an online survey. The survey proposal was approved by Institutional Review Board (IRB) and launched on Qualtrics [21].

Survey Design and Data Collection. In this survey, participants were asked to answer questions about different factors that motivate or repeal them to use COVID-19 apps. The survey questionnaires were designed to assess participants' trust, preferences, concerns towards using COVID-19 applications. The online survey solicited different types of responses in the form of multiple choices, Likert scales, Yes/No, and open-ended questions. We iteratively refined our survey, each time piloting among a small number of users to ensure the survey questions were comprehensive to people of different backgrounds.

Our online survey of COVID-19 apps was conducted between July 13, 2020, to August 13, 2020. Participants from 27 countries participated in our survey. This survey was fully voluntary, i.e., participants were not paid. Participants were all adults, above the age of 18. The survey link was distributed through the Qualtrics platform and survey data was collected by distributing the link in different social media platforms and community groups. We had a total of 357 responses, but after eliminating incomplete responses we ended up with a total of 261 responses.

4 MANUAL APP ANALYSIS

We first manually analyze the app details obtained from its official website or Google Play store or even its privacy policy to shed light on the privacy practices exercised by the app. Our analysis includes determining the data practices claimed by the apps (Section 4.1) and the extent to which they claim to be compliant with regional regulations (Section 4.2). We also analyze how the apps consider the different functional technologies available for data exchange across different geographic regions (Section 4.3).

[1]We note that some of the apps did not have their privacy policy pages in English. For the purpose of our manual analysis of data practices, we used Google Translator to have the contents translated into English [7]. For the app description page, there was an option for translating the information into English.

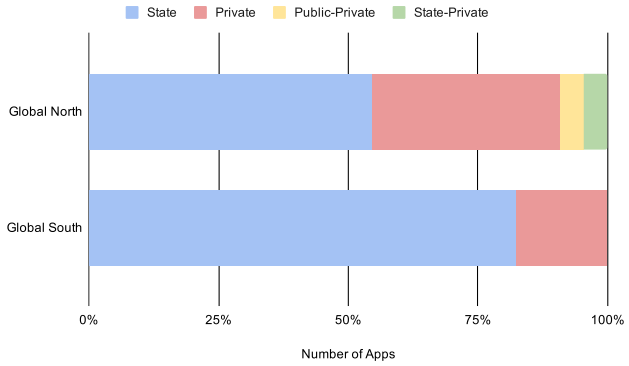

Figure 1: App Distribution by Ownership

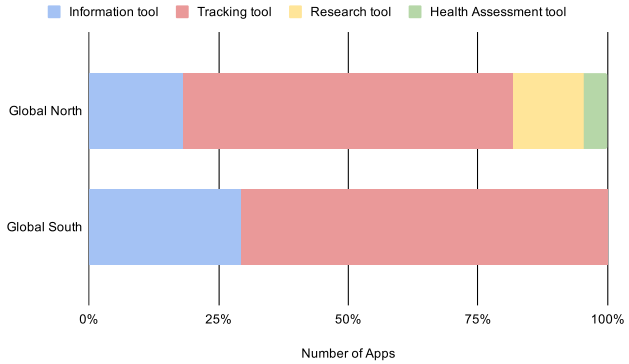

Figure 2: App Distribution by Functionality

4.1 Data practices in COVID-19 Apps

Given that a considerable number of contact-tracing apps are now being endorsed and even mandated by governments around the world, it is critical that we examine the data practices exercised by such apps. This includes understanding what data is being collected and for what purpose, with whom it is being shared and how long the data is retained. Table 1 summarizes our findings. We noticed a significant lack of transparency in data collection. Overall, 15 out of 22 apps from Global North have not mentioned transparency on data collection and storage of personal information. 14 out of 17 in Global South have not mentioned anything about data collection and transparency. Only 3 apps from Global South explicitly assert on the types of data they are collecting. Lack of transparent data collection policy can diminish the trust/confidence among end users, which can eventually lead to low engagement [32].

We noticed a comparatively good number of apps having a data processing policy: all of the apps from Global North have clearly mentioned that they have a policy for processing user data and

the reason behind those operations while in Global South it seems 7 apps did not have any policy page. We also investigated apps' data retention practices. Data retention implies the preservation of information as long as it is needed and then discarding it in a safe manner after a certain period of time. From our sample, 12 out 22 apps in Global North have data retention practices mentioned while only 4 out of 17 apps in Global South mentioned data retention practices. We are aware of the fact that companies and governments are nowadays aiming to avoid violations and strengthen customer trust by defining, and remediating data retention policies [17]. Lack of data retention policy can lower users' trust and at the same time can also cause unnecessary costs associated with storage and security (e.g., data breach) for app providers.

There was also insufficient disclosure of data sharing and distribution among different parties, where 5 out of 22 apps in Global North did not mention anything about data sharing with third parties; 9 of them mentioned they do not share data with third parties while 8 of them explicitly mentioned they shared data with certain parties. For Global South, 7 out of 17 apps mentioned sharing data with third parties, 3 of them mentioned not sharing data with third parties and 7 of them did not mention anything about data sharing. Further, we investigated the presence of opt-in/out controls for the sampled 39 COVID-19 apps. From our observation, we noticed a significant lack of user control/right over the data collected by these COVID-19 apps. We noticed 15 out of 22 apps in Global North did not have an opt-out or related features mentioned while 12 out of 17 apps in Global South did not mention anything about opt-in/out. Lastly, we investigated the presence of any statement related to regulatory compliance where 17 out of 22 in Global North mentioned having compliance and 10 out of 17 apps in Global South mentioned having compliance. Note that this analysis is solely based on statements found in an app's description or privacy policy page. More details on which regulations apps are claiming to be compliant with are available in Section 4.2.

4.2 Compliance with Regulations

During the pandemic, many COVID-19 apps have been developed within a short period of time across different regions. Different countries/regions are taking different stands considering the trade-offs between privacy and utility, often dictated by existing laws, values, attitudes, and norms. We, therefore, explore 39 apps from Global South and North to understand the landscape of regulatory practices stated by the apps.

First, we reviewed existing privacy/data protection regulations in different regions of the world. Table 2 highlights the different laws/regulations we reviewed. In terms of regulatory compliance, it seems that in Global South (countries in Asia and Africa) have some existing framework, not necessarily regulation which can be utilized effortlessly. In Global South, laws are still in the development phase (mostly based on GDPR [6]), for example, APEC [1], Asia Pacific Data Protection and Cybersecurity Regulation 2018 [2], SADC Model Law on Data Protection [49]. Some of the countries like Brazil and Colombia in the Global South recently seem to have formed data protection regulation after this pandemic [27].

In Global North (countries in Europe), the structure of data protection seems to be more established and harmonized with EU data protection law [5]. The purpose of their regulation is to provide improved privacy protection and control for EU citizens. It is designed to give individuals control of their personal data and to improve how businesses manage personal consumer data [6]. Specifically for pandemic situations, they recommend EU Toolbox for the use of technology and data to combat the COVID-19 crisis [5]. It appears to be an essential resource for an app developer to implement GDPR-compliant data practices for COVID-19 apps. In the same way, Australia-countries in Global North seem to have established data protection laws for most states and territories [47]. Unlike the harmonized compliance approach of part of Global North (EU), United Stated seems to have different types of act for different purposes, such as Health Insurance Portability and Accountability Act (HIPAA) for health data [33], Online Privacy Protection Act (OPPA) for online safety [52] and the recent California Consumer Privacy Act (CCPA) for California residents [4].

After identifying the regional privacy and data protection regulations, we examined the selected COVID-19 apps to check if they mention being compliant with specific regulations in their privacy policies. We carefully inspected the app description pages as well as the privacy policy pages to find out the laws/regulations that these apps reference to be compliant with to promote proper data practices.

In our collection, there were 6 apps from Global South that did not mention any regulatory compliance. The rest of the 11 apps has their local/country-specific privacy law and constitute. For example, NCOVI, an app from Vietnam claimed to be compliant with the provisions of Vietnamese law. The data was mentioned to be stored confidentially by their government agencies and only be used for the purpose of contact tracing. Similarly, Aarogya Setu, an app from India mentioned being compliant by clauses from the constitution of India. However, the app did not explicitly explain how data processing is being performed according to the regulation. Coronavirus UY mentioned to be compliant with Provisions of Act 843 [31] for collection and process of data; Kenya Covid-19 Tracker app claims to be compliant with Kenya's Data Protection Act for data processing where processing includes collection, storage, retrieval, dissemination of personal data or sets of personal data.

Of the 22 apps from Global North, we did not find any regulatory compliance statement for 4 apps. Other 11 apps mentioned being compliant with different sections or articles of GDPR 2016/679 [6]. For example, GDPR 2016/679 for data processing and personal data protection and GDPR-Directive 95/46/EC [6] for free movement of data. CovTracer and SOS Corona did not mention anything about particular regulatory compliance. 5 of the remaining apps mentioned to be compliant with their country-specific law, for example, Coronavirus Australia mentioned Privacy Act 1988 [3] for data processing and storage, and Australian Privacy Principles (APPs) [3] for other data practices. Lastly, 2 apps from MENA claimed to be compliant with their local regulations. Table 2 list the specific regulations that apps mention to be compliant with.

From our analysis, we see that 4 of the 22 (around 18%) Global North apps and 6 of the 17 (around 35%) Global South apps did not have any regulations explicitly referenced which shows a clear difference in perception/attitude across different regions. It seems that Global North apps either claim to be more compliant to certain

Table 1: Contrasting data practices across different regions.

Data Practice	Global North			Global South		
	Yes	No	Not Mentioned	Yes	No	Not Mentioned
Data shared with third party	8	9	5	7	3	7
Compliance	17	1	4	7	1	9
Policy page	22	0	0	10	6	1
Opt out for promotion/other services	7	0	15	3	0	12
Data retention	12	0	10	4	0	13
Data processing	17	0	5	8	0	9
Transparency in data collection	7	0	15	3	0	14

Table 2: Regulatory compliance analysis

App Name	Region	Regulations Explicitly Mentioned †	Existing Regional Laws
NCOVI	Global South	Vietnamese law	
TraceTogether	Global North	NM	Cybersecurity Regulation:2018
Aarogya Setu	Global South	The Constitution of India	GDPR
PeduliLindungi	Global South	Mentioned legal provisions	APEC
COVID-19 Gov PK	Global South	NM	Global South-Pacific Data Protection
Covid-19 Armenia	Global North	NM	
Stop COVID-19 KG	Global South	NM	
COVID19 UAE	Global South	NM	
Stop Covid-let's fight this together	Global North	Personal Data Protection-Georgia	
STOP COVID19 CAT	Global North	GDPR, Organic Law 3/2018,3/1986	
Stopp Corona	Global North	GDPR	
eRouška - part of smart quarantine	Global North	GDPR (ActNo.110/2019, Health-Service Act)	
Home Quarantine	Global North	GDPR-95/46/EC, 2016/679, Journal of Laws	
COVID Symptom Tracker	Global North	GDPR	
HSE COVID-19	Global North	Health Act 1947, GDPR	
SOS CORONA	Global North	Own created policy to avoid legal jargon	
COVID Radar	Global North	GDPR	GDPR
Castor COVID-19	Global North	NM	
Ada – your health companion	Global North	GDPR-2016/679, 95/46/EC	
COVID-19 Regione Sardegna	Global North	GDPR-2016/679	
Estamos ON-Covid19	Global North	NM	
ViruSafe	Global North	GDPR (Regulation-2016/679)	
CovTracer	Global North	Mentioned legal provisions/law (not specific)	
Rakning C-19	Global North	Icelandic Data Protection Authority	
Zostaň Zdravý	Global North	GDPR-Directive-95/46/ EC	
GH COVID-19 Tracker	Global South	Act-2012 (DPA-Act-843),Provisions of Act 843	SADC-Law on Data Protection(2010)
Coronavirus Algérie	Global South	NM	ECOWAS Supplementary Act A/SA.1/01/10
NICD COVID-19 Case Investigation	Global South	NM	EAC Framework for Cyberlaws(2008)
Kenya Covid-19 Tracker	Global South	Kenya Data Protection Act	Personal Data Protection (2010)
Coronavirus UY	Global South	Provisions of Decree No.93/020	Brazilian GDP(LGPD)
COVID-19 Provincia de Santa Fe	Global South	Argentina Personal Data Protection Law No.25,326.	ICLG Data Protection Laws
Bolivia Segura	Global South	Local:art-21,Para-2 of Political-Constitution	Mexican Data Protection Law
CoronApp-Colombia	Global South	Local law: Decree 531 of 2020	Law for Personal Data Protection-No-29733 (Peru)
Coronavirus-SUS	Global South	LGPD,provisions Law No-13709	
Coronavirus Australia	Global North	Privacy Act 1988, APPs	APPs,Privacy Act 1988
Canada COVID-19	Global North	US Privacy Act of 1974	Department of Health Act
COVID-19 Tam	Global South	NM	FTC, CCPA, HIPAA, ECPA, OPPA
BeAware Bahrain	Global South	local:Law No.(30) 2018, PDP Law	QFCData Protection Law
Korona Önlem	Global North	KVK Law No, 6698	Personal Data Protection of 2018

† NM: Not Mentioned

regulations or are more conscious about regulations. Half of the Global North apps mention General Data Protection Regulation (GDPR), while the Global South apps reference various local regulations which highlight the lack of conformity across the regions in terms of referenced regulations. We next look at the explicitly referenced regulations across the different apps.

4.3 Functional Privacy Properties

For this section, we discuss functional technology for data exchange (Bluetooth/GPS/Bluetooth+GPS), and data storage architecture (centralization/decentralization) in our sampled 39 COVID-19 apps. Out of 17 apps in Global south, 1 app uses only Bluetooth; 10 apps use

only GPS data; 3 apps use both Bluetooth and GPS, and the remaining 3 apps neither use Bluetooth or GPS data. In Global North, 3 apps use Bluetooth, 12 apps use only GPS, 1 app uses both Bluetooth and GPS, and 6 apps do not mention anything about data exchange.

Furthermore, we analyzed the data storage architecture adopted by the 39 apps to determine if data was stored in a centralized or decentralized manner, where current literature endorses the decentralized approach to enhance user privacy [55]. Only 1 app from Global South adopted decentralized data storage architecture; 5 of them adopt a centralized architecture and the rest of the apps do not mention any details about data storage architecture. Among the 17 apps from Global South, 5 apps provide COVID-19 related updates, and the rest of them are used for contact tracing. Out of 22 apps from Global North, half of them adopt a centralized and 3 of them adopt a decentralized data storage architecture, while the rest do not mention anything about the data storage architecture they adopt. 15 of these apps are used for contract tracing, 3 provide COVID-19 related updates, 3 are for research purposes, and 1 for health assessment.

In Table 4 in Appendix C, we have presented 39 apps with their functionality, storage architecture and tracking technology. We found five apps (SOS Corona, Coronavirus UY, Bolivia Segura, Coronavirus Australia, Canada COVID-19) were using tracking technology (GPS) even though their primary purpose is to only provide COVID-19 updates to citizens. Further, HSE COVID-19 was requesting GPS even though its functionality is health-related assessment.

5 USER SURVEY RESULT

In the following subsections, we present the results of our user survey.

5.1 Contextualized Factors for Study

We designed a survey with 18 questions, including both open-ended and close-ended questions. From the existing literature, it is evident that 'trust' is a diverse concept integrated into several models in the Information Systems domain [54]. Prior works also suggest that trust enables positive attitudes towards interacting with services [26]. In our current study of COVID-19 apps, we formulated several questions on trust to capture users' attitudes towards technology and technical service providers. Additionally, we focused on users' motivation about using COVID-19 apps during the time of the pandemic. Finally, we considered users' perceived privacy concerns in adopting COVID-19 apps. We report our findings along two main socio-economic divisions: the Global South and the Global North.

We hosted the survey on Qualtrics and reached out to our participants through several groups on Facebook. We utilized our professional circle to post the link to the survey in various local groups on Facebook. We acknowledge one limitation of our survey: the survey was conducted in English and as such, our sample size from the Global South represents the middle class and upper-middle-class population who are fluent in English.

5.2 User Demographics

Our sample consists of 261 participants from 27 different countries. As 14 participants did not disclose their country location, we excluded their responses. Among the remaining 247 participants, 104 (42%) were from the Global North and 143 (58%) were from the Global South.

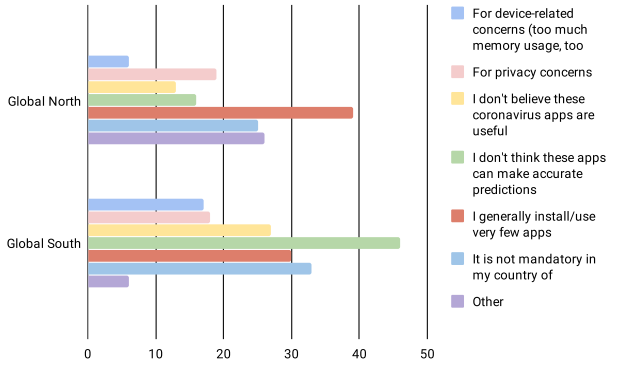

Figure 3: Why have you not used any apps related to coronavirus?

In the Global North, United States, Canada, Australia, Belgium, and Germany represented the majority of the participants. We had participants from Finland, France, Norway, Taiwan, etc., as well. A total of 55 participants were female and 47 were male and two others did not report. In the Global South, the majority of the participants were from India, Bangladesh, and Pakistan and the remaining were from American Samoa, Nigeria, South Africa, Uganda, etc. Among the 143 participants from the Global South, 73 were male and 70 were female.

5.3 User's Motivation Towards using COVID-19 Apps

Overall, 184 out of our 247 participants (74%) have not ever used any COVID-19 related mobile apps. More specifically, 72% of participants from the Global South and 76% of participants from the Global North reported having never used any COVID-19 apps. The top three reasons cited by the Global South participants were lack of confidence in the effectiveness of the apps (32%), absence of any government mandate (23%), and a general tendency towards installing very few apps (21%). The absence of government mandate (24%) and the tendency of installing very few apps were also the two top reasons (38%) for the Global North participants for not using any coronavirus-related apps. Figure 3 summarizes the reasons for not using any apps related to COVID-19.

We also looked into the responses of the rest of the participants (26%) who have used COVID-19 apps as they were asked to describe their motivations to use COVID-19 apps. For both regions, we got similar top three responses: "Well-being of myself and my family", "Instruction from the government", and "curiosity" (see Figure 4).

To form additional understanding, we asked an open-ended question to participants who used COVID-19 apps regarding what led them to the decision to download and use those apps. Their responses reflected that sense of responsibility towards the community was the major reason for them to install and use those apps. Two typical responses were as following:

> "*I did not really have concerns. The apps weren't very invasive as far as privacy is concerned and even if they were doing things like tracking my location, I think it's*

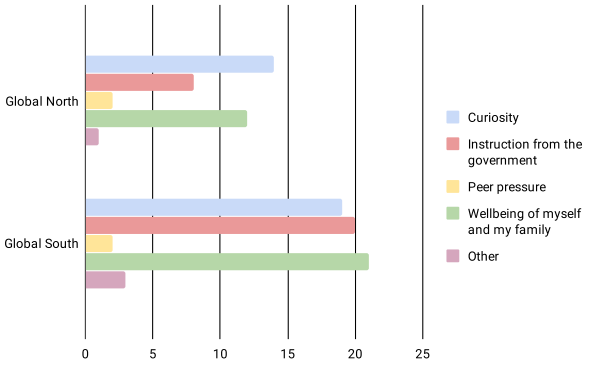

Figure 4: What made you install the app?

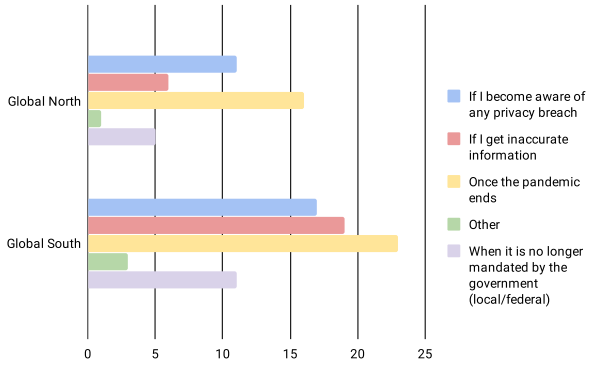

Figure 5: Under what circumstances would you delete the app?

worth it to help better equip my community to tackle COVID." (The Global North)

"*There was not any particular concern, just a sense of responsibility led me to download the app.*" (The Global South)

There were also a few responses that reflected a positive attitude towards technology. One such response was as following:

"*The app informed me about the current availability of hospitals (beds/ventilators) along with their location so it was a source of valuable information.*"

This suggests that for the participants who decided to use the COVID-19 apps, a sense of responsibility trumped their privacy concerns.

5.4 Users' Privacy Concerns

From our survey, we observed that the most frequently used COVID-19 apps were coronavirus apps that provide information (38% of total responses), i.e., map, visualization, etc. The second most frequently used app was contract-tracing apps (30%), followed by self-assessment apps (25%) that check symptoms. For the Global South, information apps were the top category whereas in the Global North, the most frequently used type was contact-tracing apps (as shown in Figure 6).

To understand the privacy concerns around COVID-19 app usage, we asked the possible circumstances under which they would delete the apps. Overall, 35% answered that they would do that after the end of the pandemic, 25% participants replied that they would only delete if they become aware of any privacy breach, and 24% said that they would do so if they find inaccurate information (Figure 5). It was evident from the responses that the Global North (28%) participants were more concerned about privacy breaches than those from the Global South (22%). The Global South responses were also leaned towards "Once the pandemic ends" (32%) and getting "inaccurate information" (26%) (see Figure 5).

We also asked the participants what would reduce their concerns in using a COVID-19 app through an open-ended question. We found that not all the responses were self-explanatory or relevant to the questions and thus discarded such responses (18%). We performed a thematic analysis on the rest of the responses and found the following themes: *nothing can reduce concerns*, *no concerns*, *privacy benchmark/assurance*, *health safety*, *functional requirement*, *transparent data policy/ more information*, *accuracy/ relevance*, *data handled by trusted entity*, and *peer recommendation*.

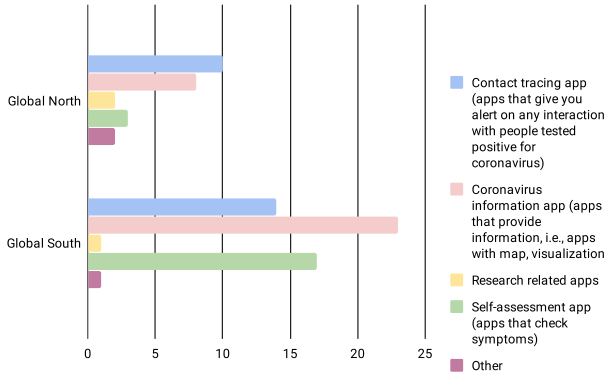

Figure 6: What type of coronavirus related app are you using?

One participant said:

"An explanation of how its results are going to be used by taking into account the limitations of the technology – this would be very much convincing to me. Also, I would like to see a clear link between the app and the platform used to implement it (e.g., DP3T)." (the Global North)

Even if privacy benchmarks and transparency in data policy are ensured, many participants can not trust the app unless its data is handled by a trusted entity. In participant's words:

"If the data is being handled by a company I trust and they maintain anonymity, I will probably use it" (the Global North)

Interestingly, some of the responses revealed people's lack of trust in government entities. They think that if an app is somehow connected to the government, there is a chance of data being exploited. In participant's words:

"Knowing that it is not connected to anyone in the government or anyone being monetarily benefited from COVID-19 is important to me." (the Global North)

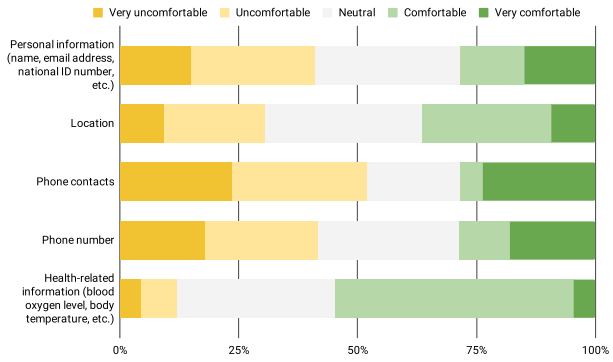

Figure 7: Different information sharing with a COVID-19 app (the Global South)

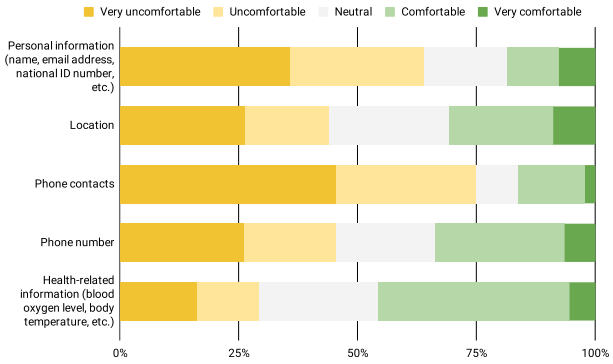

Figure 8: Different information sharing with a COVID-19 app (the Global North)

A good number of responses, mostly from the countries of the Global South, revealed the fact that a lot of people have not heard about COVID-19 apps.

5.5 Users' Privacy Preferences

To have an understanding of privacy preferences, our survey questions asked about users' opinions in sharing different personal information via COVID-19 apps. We know that different types of COVID-19 apps require a substantial amount of information for fulfilling specific purposes. For example, contact tracing apps require location or Bluetooth information to provide exposure notification, self assessment apps often require health-related information to recommend appropriate measures. Figure 7 and Figure 8 present different data sharing preferences for the Global South and the Global North users, respectively.

We further asked the participants to rate their comfort in obtaining tracing information by smartphone manufacturers via COVID-19 contact tracing apps. We found that 38% of the participants from the Global North and 42% of the participants from the Global South were comfortable. We also asked them to rate how comfortable they would be when the mobile operating system would start sharing this contact tracing data with different entities if they test positive for coronavirus. There was a major difference in the responses

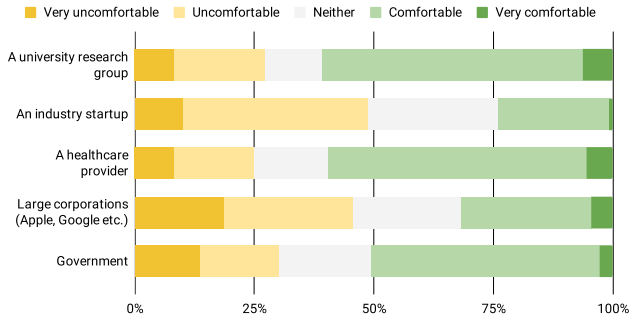

Figure 9: Comfort rating in sharing tracing data with different entities (the Global South)

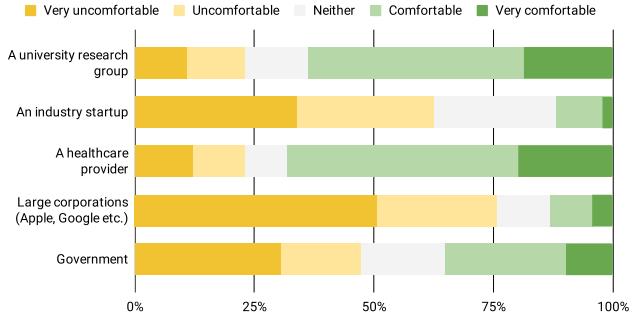

Figure 10: Comfort rating in sharing tracing data with different entities (the Global North)

from the Global North and the Global South in case of rating for large corporations such as Google and Apple. The Global North participants were more reluctant in data sharing with large corporations than those of the Global South. At the same time, there was a similarity between the Global North and the Global South users in their preferences towards university research groups and healthcare providers in case of sharing the tracing data. Figure 9 and Figure 10 present ratings for these two types of entities.

We also asked the participants an open-ended question about any other privacy concerns related to COVID-19 apps. Most of the responses were related to data privacy and data practices. Some users told that they would use the app only if it ensured data privacy and followed certain data practices. They pointed out the issue of data sharing with third parties. From the responses, it seems like that the Global North users are more aware of individual rights and they think of it as a threat to their rights. There were some exceptions though. For example, one participant suggested that COVID-19 apps should be used for greater good and health safety:

"I wish they had been used in the US. I think the general population has made mistakes in caring more about individual rights than community health and well-being." (the Global North)

Participants also mentioned their preferences for functional requirements of COVID-19 apps such as less power consumption, easy-to-use interface, and exemption from repetitive messages, etc. Some of them explicitly mentioned the issue of data retention/deletion. In participant's words:

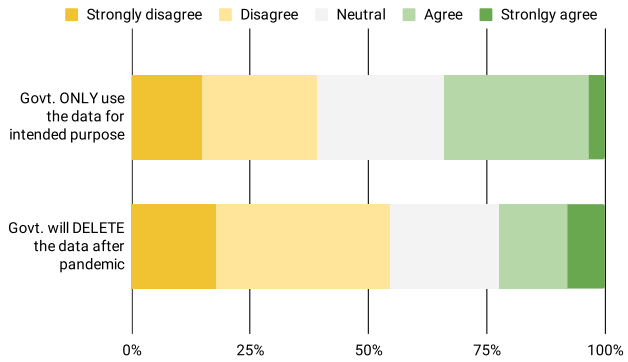

Figure 11: Trust regarding government would only use collected data for the intended purpose (the Global South)

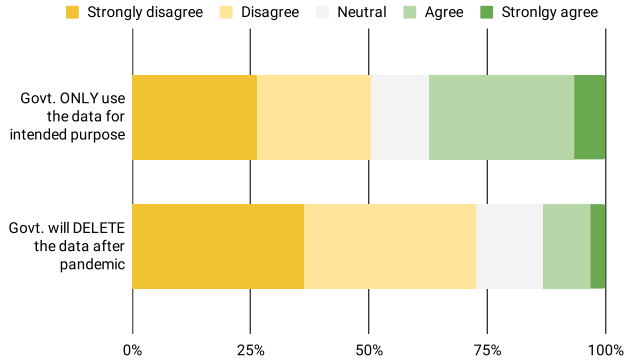

Figure 12: Trust regarding government would only use collected data for the intended purpose (the Global North)

"I would like to state that as long as there comes a guarantee that the collected data from every individual would be destroyed after the purpose, then it would create no harm." (the Global North)

One participant's response indicated a comparison between the regular apps and the coronavirus mitigation apps:

"Different industries/governments collect our personal data through our social media or other apps installed in our devices already. I don't think a COVID-19 app would create a bigger problem for privacy." (the Global North)

5.6 Users' Trust and Transparency

In comparison to the Global South users, the Global North users have less trust in their government regarding the collection and protection of COVID-19 related data. Figures 11 and 12 summarize their responses in this regard. Additionally, both user groups tend to trust university research groups and healthcare providers more than industry startups and large corporations for protecting user data collected through a COVID-19 app (as evident in Figure 13 and Figure 14). For example, one participant expressed concerns for data retention explicitly.

"Usually I do not prefer my contact or location with my own family members with whom I am uncomfortable with but due to this pandemic if we all are not together and not use the technological advantage to fight with covid then we are in a bigger loss. I would like to state that as long as there comes a guarantee that the data that has been collected from every individual is destroyed after the purpose then it would create no harm."

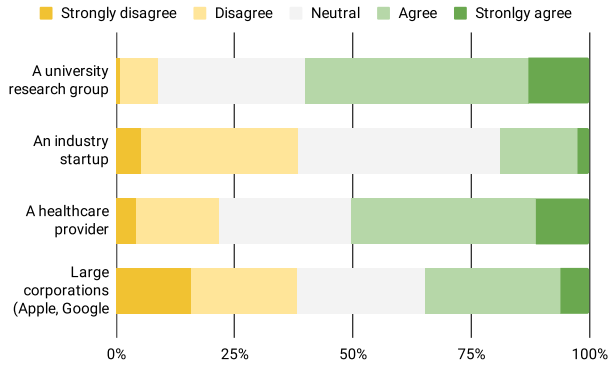

Figure 13: Entities would protect user data collected through a COVID-19 app (the Global South)

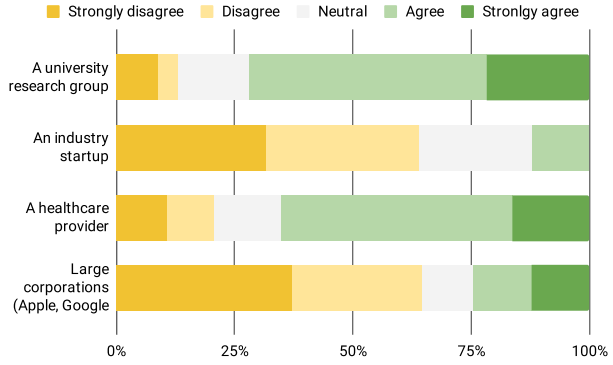

Figure 14: Entities would protect user data collected through a COVID-19 app (the Global North)

6 DISCUSSION

In recent years, mitigating the COVID-19 pandemic has been the primary agenda for the global community, and smartphone app developers have been playing a vital role in this regard. Mobile devices present an ideal platform to combat COVID-19 due to their availability and personalized usage patterns. Therefore, several smartphone apps have been deployed by governments, international agencies, and other parties to mitigate the spread of the virus. However, there is an increasing concern regarding the collection and storage of data, and outsourcing data to third-party systems. In this paper, we analyzed a large set of COVID-19 apps from two different regions (Global South and Global North) with respect to different security and privacy metrics. Specifically, we examined those apps for their data practices, compliance with regulations, and user perception during app usage.

Our study presents similarities, differences, and notable findings from different regions of the world. First, with app analysis

of COVID-19 apps, we became aware of the transparency and privacy protection loopholes of the apps. Notably, most of the apps did not have transparent data processing method as well as clear description about data collection strategies. Many apps did not have a data retention policy and some of the apps had limited user control/right over data and many of those did not comply with regulations. Moreover, very few apps followed data encryption mechanisms while allowing data exchange through Bluetooth and GPS, which can cause unwanted data leakage from a user's phone. Our major findings are as follows:

- There remains a considerable difference in different regions of the world in terms of technological, social, economical, and political structure. Unlike the Global North, there exists a lack of well-regulated policies and laws in the Global South. We have noticed that a good number of COVID-19 apps from those regions (7 out of 17 apps in Global South) do not mention being compliant with regulations for the purpose of processing and handling user data. We note that the majority of our selected COVID-19 apps require certain types of data, including health and location information to offer the basic functionality of tracking/assessment. In the case of Global North, we have seen that the majority of apps are compliant with regulations for data processing. Some of them (four) include additional regulations for the protection of personal data (e.g., Health Service Act for health data) and to provide the guarantee of protection for COVID-19 related health information as well. This fact is linked to the reality that law enforcement agencies and regulatory bodies are more powerful in this region. For the same reason, the availability of data retention policy and app policy page is higher for apps in Europe.
- The majority of apps from Global South did not adopt appropriate security measures for the exchange of data to and from the user to the data centers. Perhaps, it might be a result of not having proper privacy/security frameworks and guidelines exercised in that part of the world. Furthermore, in the case of deployment framework for data center and sensor technology, we have found issues in apps from both the Global South and North. For example, Stop Corona and Aarogya Setu use Bluetooth as their tracing technology and their Broadcast Receiver service was left accessible to other apps on a user's device.

Furthermore, from the user survey, we have found different perspectives around users' trust, preferences, concerns, and sense of usefulness of technology.

- In the case of usefulness, the majority of participants from the Global South seem not to think the apps can function accurately which seemed to be the top reason for not using COVID-19 apps. However, from Global North's response, we could not get the notion of the COVID-19 app as not being useful. There were similar impressions on COVID-19 apps' usefulness due to the well-being of themselves and their family for both the Global South and North population. Even open-ended responses express a positive attitude towards COVID-19 apps due to health safety and greater good as well as a sense of responsibility for the community. Though responses showed the usefulness of these apps, there still remain concerns around using COVID-19 apps.
- Both the Global South and North expressed that they would delete the apps once the pandemic end and if they are aware of any privacy breach and get any information inaccurate. To be noted that the Global South responses had fewer privacy breach concerns than the Global North. We found a closely aligned overarching theme from open-ended responses. There were frequent responses from open-ended questions that deliberate concerns for lack of proper privacy benchmark as well as transparent data policy and lack of functional accuracy.
- We have found that participants had some preferences while it comes to share different types of information with COVID-19 apps. We have seen that both the Global North and South population are very uncomfortable sharing phone contact with COVID-19 apps. In addition, we have seen that the Global North seems to be more reluctant to share personal information and location than the Global South.
- In case of trust in app providers and their governments in handling data, we noted Global North and South majority population is trusting in university research groups and healthcare providers more than any large corporation and industry. Also, both Global North and South do not believe that the government of their country will delete all the collected data via the COVID-19 app after the pandemic. However, they seem to trust that government will use those data for intended purposes only.

Mobile applications have been playing a prominent role in addressing the current pandemic challenges and in the containment of the spread of the virus. However, the effectiveness and accuracy of these systems depend upon the working architecture of applications for ensuring security and maintaining public trust. To ensure privacy and security and secure development of COVID-19 apps, we recommend the following design choices:

- In order to ensure the privacy and security of user data, COVID-19 apps need to be compliant with the minimum requirement for data processing and safeguarding health data. In this case, an ideal suggestion would be 'data minimalism' which can promote the idea that developers should try to obtain the least amount of data required for the main functionalities provided by apps. More specifically, the design system should not unnecessarily seek permissions for certain information which are not related to their functionalities, for example, access to videos, browsing history, or images.
- The app's privacy policy on the collection, use, and sharing of personal information should be effortlessly perceptible for COVID-19 app users. A guideline can be articulated for app developers that include mandatory criteria associated with privacy, i.e., implementing security safeguards for deployment framework, data minimization, limiting use and disclosure on data retention, stating the clear purpose of data handling, mechanisms for consent, and controls for users.
- Since we have found different issues related to deployment architecture (centralized/decentralized), in this case, developers should consider the semantics of secure software

development including secure communication mechanisms for the exchange of data between the users and the data center. Furthermore, there is a big concern in our findings regarding data practices on how and when data will be deleted. To address this issue, particularly for pandemic situations, there needs to be a mechanism for users to easily destroy the data once the pandemic situation is over.

In this study, we conducted a manual and static analysis to report privacy vulnerabilities, inconsistencies, and lack of regulatory compliance of COVID-19 apps. One possible future direction of work could be to conduct a comprehensive global survey on end-users and app developers to understand their perceptions about these apps. The responses to the survey would complement the findings that have been reported in this study.

REFERENCES

[1] 2020. *APEC Privacy Framework*. www.apec.org/Publications/2017/08/APEC
[2] 2020. *Asia Pacific Data Protection and Cyber Security Guide 2019*. http://documents.jdsupra.com/2380c6d9-41fd-48bb-9f78-3fba5aa25e52.pdf
[3] 2020. *Australian Privacy Principles*. https://www.oaic.gov.au/privacy/australian-privacy-principles/
[4] 2020. California Consumer Privacy Act (CCPA). https://oag.ca.gov/privacy/ccpa.
[5] 2020. *European Data Protection Board*. https://edpb.europa.eu/sites/edpb/
[6] 2020. *General Data Protection Regulation*. https://gdpr-info.eu/
[7] 2020. *Google Translator*. https://translate.google.com/?ui=tob
[8] 2020. *Privacy Act of 1974*. https://it.ojp.gov/PrivacyLiberty/authorities/statutes/1279
[9] 2021. About the Sustainable Development Goals - United Nations Sustainable Development. https://www.un.org/sustainabledevelopment/sustainable-development-goals/
[10] 2021. Ensure healthy lives and promote well-being for all at all ages. https://sdgs.un.org/goals/goal3
[11] Nadeem Ahmed, Regio A Michelin, Wanli Xue, Sushmita Ruj, Robert Malaney, Salil S Kanhere, Aruna Seneviratne, Wen Hu, Helge Janicke, and Sanjay K Jha. 2020. A survey of covid-19 contact tracing apps. *IEEE Access* 8 (2020), 134577–134601.
[12] Syed Ishtiaque Ahmed, Shion Guha, Md Rashidujjaman Rifat, Faysal Hossain Shezan, and Nicola Dell. 2016. Privacy in repair: An analysis of the privacy challenges surrounding broken digital artifacts in bangladesh. In *Proceedings of the Eighth International Conference on Information and Communication Technologies and Development*. 1–10.
[13] Syed Ishtiaque Ahmed, Md Romael Haque, Jay Chen, and Nicola Dell. 2017. Digital privacy challenges with shared mobile phone use in Bangladesh. *Proceedings of the ACM on Human-Computer Interaction* 1, CSCW (2017), 1–20.
[14] Syed Ishtiaque Ahmed, Md Romael Haque, Shion Guha, Md Rashidujjaman Rifat, and Nicola Dell. 2017. Privacy, security, and surveillance in the Global South: A study of biometric mobile SIM registration in Bangladesh. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*. 906–918.
[15] Syed Ishtiaque Ahmed, Md Romael Haque, Irtaza Haider, Jay Chen, and Nicola Dell. 2019. " Everyone Has Some Personal Stuff" Designing to Support Digital Privacy with Shared Mobile Phone Use in Bangladesh. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. 1–13.
[16] Syed Ishtiaque Ahmed, Steven J Jackson, Nova Ahmed, Hasan Shahid Ferdous, Md Rashidujjaman Rifat, ASM Rizvi, Shamir Ahmed, and Rifat Sabbir Mansur. 2014. Protibadi: A platform for fighting sexual harassment in urban Bangladesh. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. 2695–2704.
[17] Esma Aïmeur, Oluwa Lawani, and Kimiz Dalkir. 2016. When changing the look of privacy policies affects user trust: An experimental study. *Computers in Human Behavior* 58 (2016), 368–379.
[18] Mahdi Nasrullah Al-Ameen, Tanjina Tamanna, Swapnil Nandy, MA Manazir Ahsan, Priyank Chandra, and Syed Ishtiaque Ahmed. 2020. We Don't Give a Second Thought Before Providing Our Information: Understanding Users' Perceptions of Information Collection by Apps in Urban Bangladesh. In *Proceedings of the 3rd ACM SIGCAS Conference on Computing and Sustainable Societies*. 32–43.
[19] Bethania de Araujo Almeida, Danilo Doneda, Maria Yury Ichihara, Manoel Barral-Netto, Gustavo Correa Matta, Elaine Teixeira Rabello, Fabio Castro Gouveia, and Mauricio Barreto. 2020. Personal data usage and privacy considerations in the COVID-19 global pandemic. *Ciência & Saúde Coletiva* 25 (2020), 2487–2492.
[20] Samuel Altmann, Luke Milsom, Hannah Zillessen, Raffaele Blasone, Frederic Gerdon, Ruben Bach, Frauke Kreuter, Daniele Nosenzo, Séverine Toussaert, and Johannes Abeler. 2020. Acceptability of app-based contact tracing for COVID-19: Cross-country survey study. *JMIR mHealth and uHealth* 8, 8 (2020), e19857.
[21] Robert J Amdur and Elizabeth A Bankert. 2010. *Institutional review board member handbook*. Jones & Bartlett Publishers.
[22] Muhammad Ajmal Azad, Junaid Arshad, Syed Muhammad Ali Akmal, Farhan Riaz, Sidrah Abdullah, Muhammad Imran, and Farhan Ahmad. 2020. A First Look at Privacy Analysis of COVID-19 Contact Tracing Mobile Applications. *IEEE Internet of Things Journal* (2020).
[23] Steven Bellman, Eric J Johnson, Stephen J Kobrin, and Gerald L Lohse. 2004. International differences in information privacy concerns: A global survey of consumers. *The Information Society* 20, 5 (2004), 313–324.
[24] Samuel Brack, Leonie Reichert, and Björn Scheuermann. 2020. Decentralized Contact Tracing Using a DHT and Blind Signatures. *IACR Cryptol. ePrint Arch.* 2020 (2020), 398.
[25] Jobie Budd, Benjamin S Miller, Erin M Manning, Vasileios Lampos, Mengdie Zhuang, Michael Edelstein, Geraint Rees, Vincent C Emery, Molly M Stevens, Neil Keegan, et al. 2020. Digital technologies in the public-health response to COVID-19. *Nature medicine* 26, 8 (2020), 1183–1192.
[26] Lemuria Carter and France Bélanger. 2005. The utilization of e-government services: citizen trust, innovation and acceptance factors. *Information systems journal* 15, 1 (2005), 5–25.
[27] Fernando Nobre Cavalcante. 2020. "Alexa, What about LGPD?": The Brazilian Data Protection Regulation in the C ontext of the Mediatization of Virtual Assistants. *Security and Privacy in the Internet of Things* (2020), 151.
[28] Justin Chan, Shyam Gollakota, Eric Horvitz, Joseph Jaeger, Sham Kakade, Tadayoshi Kohno, John Langford, Jonathan Larson, Sudheesh Singanamalla, Jacob Sunshine, et al. 2020. Pact: Privacy sensitive protocols and mechanisms for mobile contact tracing. *arXiv preprint arXiv:2004.03544* (2020).
[29] Hyunghoon Cho, Daphne Ippolito, and Yun William Yu. 2020. Contact tracing mobile apps for COVID-19: Privacy considerations and related trade-offs. *arXiv preprint arXiv:2003.11511* (2020).
[30] D Cooper, KV Quathem, and AO Meneses. [n.d.]. COVID-19 Apps and Websites–The "Pan-European Privacy Preserving Proximity Tracing Initiative" and Guidance by Supervisory Authorities.
[31] Dominic N Dagbanja. 2016. The right to privacy and data protection in Ghana. In *African Data Privacy Laws*. Springer, 229–248.
[32] Judy Drennan, Gillian Sullivan, and Josephine Previte. 2006. Privacy, risk perception, and expert online behavior: An exploratory study of household end users. *Journal of Organizational and End User Computing (JOEUC)* 18, 1 (2006), 1–22.
[33] Peter Edemekong, Pavan Annamaraju, and Micelle Haydel. 2020. Health Insurance Portability and Accountability Act. *StatPearls* (2020).
[34] Robert A Fahey and Airo Hino. 2020. COVID-19, digital privacy, and the social limits on data-focused public health responses. *International Journal of Information Management* 55 (2020), 102181.
[35] Felix Fischer, Konstantin Böttinger, Huang Xiao, Christian Stransky, Yasemin Acar, Michael Backes, and Sascha Fahl. 2017. Stack overflow considered harmful? the impact of copy&paste on android application security. In *2017 IEEE Symposium on Security and Privacy (SP)*. IEEE, 121–136.
[36] Urs Gasser, Marcello Ienca, James Scheibner, Joanna Sleigh, and Effy Vayena. 2020. Digital tools against COVID-19: taxonomy, ethical challenges, and navigation aid. *The Lancet Digital Health* (2020).
[37] Sara Gerke, Carmel Shachar, Peter R Chai, and I Glenn Cohen. 2020. Regulatory, safety, and privacy concerns of home monitoring technologies during COVID-19. *Nature medicine* 26, 8 (2020), 1176–1182.
[38] Katherine Gnadinger. 2014. The Apps Act: Regulation of Mobile Application Privacy. *SMU Sci. & Tech. L. Rev.* 17 (2014), 415.
[39] Kyra H Grantz, Hannah R Meredith, Derek AT Cummings, C Jessica E Metcalf, Bryan T Grenfell, John R Giles, Shruti Mehta, Sunil Solomon, Alain Labrique, Nishant Kishore, et al. 2020. The use of mobile phone data to inform analysis of COVID-19 pandemic epidemiology. *Nature communications* 11, 1 (2020), 1–8.
[40] SM Taiabul Haque, MD Romael Haque, Swapnil Nandy, Priyank Chandra, Mahdi Nasrullah Al-Ameen, Shion Guha, and Syed Ishtiaque Ahmed. 2020. Privacy Vulnerabilities in Public Digital Service Centers in Dhaka, Bangladesh. In *Proceedings of the 2020 International Conference on Information and Communication Technologies and Development*. 1–12.
[41] SM Taiabul Haque, Pratyasha Saha, Muhammad Sajidur Rahman, and Syed Ishtiaque Ahmed. 2019. Of Ulti,'hajano', and" Matachetar otanetak datam" Exploring Local Practices of Exchanging Confidential and Sensitive Information in Urban Bangladesh. *Proceedings of the ACM on Human-Computer Interaction* 3, CSCW (2019), 1–22.
[42] Farkhondeh Hassandoust, Saeed Akhlaghpour, and Allen C Johnston. 2021. Individuals' privacy concerns and adoption of contact tracing mobile applications in a pandemic: a situational privacy calculus perspective. *Journal of the American Medical Informatics Association* 28, 3 (2021), 463–471.
[43] Anurag Kumar Jain and Devendra Shanbhag. 2012. Addressing security and privacy risks in mobile applications. *IT Professional* 14, 5 (2012), 28–33.
[44] Maya Krishnan. 2015. Survey on Security Risks in Android OS and an Introduction to Samsung KNOX. *International Journal of Computer Science and Information Technologies* 6, 4 (2015), 3965–3967.

[45] Naomi Lefkovitz and Kaitlin Boeckl. 2020. NIST Privacy Framework: An Overview. (2020).
[46] Jinfeng Li and Xinyi Guo. 2020. COVID-19 Contact-tracing Apps: A Survey on the Global Deployment and Challenges. *arXiv preprint arXiv:2005.03599* (2020).
[47] David Lindsay. 2005. An exploration of the conceptual basis of privacy and the implications for the future of Australian privacy law. *Melb. UL Rev.* 29 (2005), 131.
[48] Joseph K Liu, Man Ho Au, Tsz Hon Yuen, Cong Zuo, Jiawei Wang, Amin Sakzad, Xiapu Luo, and Li Li. 2020. Privacy-Preserving COVID-19 Contact Tracing App: A Zero-Knowledge Proof Approach. *IACR Cryptol. ePrint Arch.* 2020 (2020), 528.
[49] Alex Boniface Makulilo. 2012. Privacy and data protection in Africa: a state of the art. *International Data Privacy Law* 2, 3 (2012), 163–178.
[50] Katina Michael and Roba Abbas. 2020. Behind COVID-19 contact trace apps: the Google–Apple partnership. *IEEE Consumer Electronics Magazine* 9, 5 (2020), 71–76.
[51] Fayika Farhat Nova, MD Rashidujjaman Rifat, Pratyasha Saha, Syed Ishtiaque Ahmed, and Shion Guha. 2019. Online sexual harassment over anonymous social media in Bangladesh. In *Proceedings of the Tenth International Conference on Information and Communication Technologies and Development*. 1–12.
[52] Gregory Shaffer. 2000. Globalization and social protection: the impact of EU and international rules in the ratcheting up of US privacy standards. *Yale J. Int'l L.* 25 (2000), 1.
[53] Lucy Simko, Ryan Calo, Franziska Roesner, and Tadayoshi Kohno. 2020. COVID-19 Contact Tracing and Privacy: Studying Opinion and Preferences. *arXiv preprint arXiv:2005.06056* (2020).
[54] Amrit Tiwana and Ephraim R McLean. 2005. Expertise integration and creativity in information systems development. *Journal of management information systems* 22, 1 (2005), 13–43.
[55] Carmela Troncoso, Mathias Payer, Jean-Pierre Hubaux, Marcel Salathé, James Larus, Edouard Bugnion, Wouter Lueks, Theresa Stadler, Apostolos Pyrgelis, Daniele Antonioli, et al. 2020. Decentralized privacy-preserving proximity tracing. *arXiv preprint arXiv:2005.12273* (2020).
[56] Robert Walters, Leon Trakman, and Bruno Zeller. 2019. *Data protection law: A comparative analysis of Asia-Pacific and European approaches*. Springer Nature.
[57] Haohuang Wen, Qingchuan Zhao, Zhiqiang Lin, Dong Xuan, and Ness Shroff. 2020. 'A study of the privacy of COVID-19 contact tracing apps. In *International Conference on Security and Privacy in Communication Networks*.
[58] Simon N Williams, Christopher J Armitage, Tova Tampe, and Kimberly Dienes. 2020. Public attitudes towards COVID-19 contact tracing apps: A UK-based focus group study. *Health Expectations* (2020).
[59] Demetrios Zeinalipour-Yazti and Christophe Claramunt. 2020. Covid-19 mobile contact tracing apps (mcta): A digital vaccine or a privacy demolition?. In *2020 21st IEEE International Conference on Mobile Data Management (MDM)*. IEEE, 1–4.
[60] Melvyn Zhang, Aloysius Chow, and Helen Smith. 2020. COVID-19 Contact-Tracing Apps: Analysis of the Readability of Privacy Policies. *Journal of Medical Internet Research* 22, 12 (2020), e21572.

APPENDIX

A KEYWORDS USED TO SEARCH APPS

"COVID-19 app", "coronavirus app", "COVID-19 Tracking", "COVID-19 contact tracing", "Pandemic app", "COVID-19", "Contact Tracing", "COVID app", "covid19 app", "covid-19".

B COVID-19 APPS ANALYZED

Table 3: Apps analyzed

App Name	Country	App Source
NCOVI	Vietnam	https://play.google.com/store/apps/details?id=com.vnptit.innovation.ncovihl=None
TraceTogether	Singapore	https://play.google.com/store/apps/details?id=sg.gov.tech.bluetrace
Aarogya Setu	India	https://play.google.com/store/apps/details?id=nic.goi.aarogyasetu
PeduliLindungi	Indonesia	https://play.google.com/store/apps/details?id=com.telkom.tracencar
COVID-19 Gov PK	Pakistan	https://play.google.com/store/apps/details?id=com.govpk.covid19
Covid-19 Armenia	Armenia	https://play.google.com/store/apps/details?id=am.gov.covid19\hl=None
Stop COVID-19 KG	Kyrgyzstan	https://play.google.com/store/apps/details?hl=en\id=kg.cdt.stopcovid19
COVID19 UAE	UAE	https://play.google.com/store/apps/details?id=com.knasirayaz.mohapcovid
Stop Covid-let's fight this together	Georgia	https://play.google.com/store/apps/details?id=gov.georgia.novid20\hl=None
STOP COVID19 CAT	Spain	https://play.google.com/store/apps/details?id=cat.gencat.mobi.StopCovid19Cat
Stopp Corona	Austria	https://play.google.com/store/apps/details?id=at.roteskreuz.stopcorona
eRouška - part of smart quarantine	Czech Republic	https://play.google.com/store/apps/details?hl=en\id=cz.covid19cz.erouska
Home Quarantine	Poland	https://play.google.com/store/apps/details?id=pl.nask.droid.kwarantannadomowa\hl=en_US
COVID Symptom Tracker	UK	https://play.google.com/store/apps/details?id=com.joinzoe.covid_zoe\hl=None
HSE COVID-19	Ireland	https://play.google.com/store/apps/details?id=com.maithu.transplantbuddy.covid19\hl=en\gl=us
SOS CORONA	France	https://play.google.com/store/apps/details?id=io.ageticmali.soscovid\hl=None
COVID Radar	Netherlands	https://play.google.com/store/apps/details?id=nl.lumc.covidradar\hl=None
Castor COVID-19	Netherlands	https://play.google.com/store/apps/details?id=com.castoredc.covid19\hl=None
Ada – your health companion	Germany	https://play.google.com/store/apps/details?id=com.ada.app\hl=None
COVID-19 Regione Sardegna	Sardinia Region	https://play.google.com/store/apps/details?id=it.regione.sardegna.modulicovid19\hl=None
Estamos ON-Covid19	Portugal	https://play.google.com/store/apps/details?id=com.vost.covid19mobile\hl=None
ViruSafe	Bulgaria	https://play.google.com/store/apps/details?id=bg.government.virusafe
CovTracer	Cyprus	https://play.google.com/store/apps/details?id=edu.rise.ihnilatis
Rakning C-19	Iceland	https://play.google.com/store/apps/details?id=is.landlaeknir.rakning\hl=en_GB
Zostaň Zdravý	Slovak Republic	https://play.google.com/store/apps/details?id=sk.marekgogol.zostanzdravy
GH COVID-19 Tracker	Ghana	https://play.google.com/store/apps/details?id=com.moc.gh\hl=en\gl=us
Coronavirus Algérie	Algeria	https://play.google.com/store/apps/details?id=com.covid19_algeria\hl=None
NICD COVID-19 Case Investigation	South Africa	https://play.google.com/store/apps/details?id=com.NICD.contactTracer\hl=None
Kenya Covid-19 Tracker	Kenya	https://play.google.com/store/apps/details?id=org.medicmobile.webapp.mobile.surveillance_covid19_kenya
Coronavirus UY	Uruguay	https://play.google.com/store/apps/details?id=uy.gub.salud.plancovid19uy\hl=None
COVID-19 Provincia de Santa Fe	Argentina	https://play.google.com/store/apps/details?id=ar.gov.santafe.mobile.coronavirusapp\hl=None
Bolivia Segura	Bolivia	https://play.google.com/store/apps/details?id=com.agetic.coronavirusapp
CoronApp-Colombia	Colombia	https://play.google.com/store/apps/details?id=co.gov.ins.guardianes\hl=None
Coronavirus Australia	Australia	https://play.google.com/store/apps/details?id=au.gov.health.covid19\hl=None
Coronavirus-SUS	Brazil	https://play.google.com/store/apps/details?id=br.gov.datasus.guardioes\hl=None
Canada COVID-19	Canada	https://play.google.com/store/apps/details?id=ca.gc.hcsc.canada.covid19\hl=None
COVID-19 Tam	Mexico	https://play.google.com/store/apps/details?id=mx.gob.tamaulipas.covid19
BeAware Bahrain	Bahrain	https://play.google.com/store/apps/details?id=bh.bahrain.corona.tracker
Korona Önlem	Turkey	https://play.google.com/store/apps/details?id=tr.gov.saglik.koronaonlem\hl=en\gl=us

C PRIVACY PROPERTIES OF APPS

Table 4: App functional properties

App	Region	Arch.	Tracing.T	Func	DC	DP	DS	DR	Trackers
NCOVI	Global South	NA	NA	Info.T.	NM	Y	N	NM	1
TraceTogether	Global North	Centralized	Bluetooth	Track.T.	Y	Y	N	Y	3
Aarogya Setu	Global South	Centralized	GPS+BL	Track.T	Y	NM	N	NM	4
PeduliLindungi	Global South	Decentralized	Bluetooth	Track.T.	NM	Y	NM	NM	2
COVID-19 Gov PK	Global South	NA	GPS	Track.T.	NM	NM	Y	NM	0
Covid-19 Armenia	Global North	Centralized	NA	Track.T.	NM	Y	N	NM	1
Stop COVID-19 KG	Global South	Centralized	GPS	Track.T.	Y	Y	N	NM	1
COVID19 UAE	Global South	Centralized	GPS	Track.T.	NM	Y	Y	Y	1
Stop Covid-let's fight this together	Global North	Centralized	GPS+BL	Track.T.	Y	Y	Y	Y	7
STOP COVID19 CAT	Global North	Centralized	GPS	Track.T.	NM	Y	NM	NM	1
Stopp Corona	Global North	Decentralized	Bluetooth	Track.T.	NM	Y	N	Y	2
eRouška - part of smart quarantine	Global North	Decentralized	Bluetooth	Track.T.	Y	Y	Y	Y	1
Home Quarantine	Global North	NA	GPS	Track.T.	NM	Y	N	NM	2
COVID Symptom Tracker	Global North	NA	NA	Research.T	Y	Y	Y	Y	0
HSE COVID-19	Global North	Centralized	GPS	H.Assess.T	Y	Y	Y	Y	1
SOS CORONA	Global North	NA	GPS	Info.T.	Y	Y	Y	Y	1
COVID Radar	Global North	NA	NA	Research	Y	NM	NM	Y	4
Castor COVID-19	Global North	NA	NA	Research.T.	Y	Y	Y	Y	1
Ada – your health companion	Global North	Centralized	GPS	Track.T.	Y	Y	Y	Y	10
COVID-19 Regione Sardegna	Global North	NA	NA	Track.T.	Y	Y	Y	Y	4
Estamos ON-Covid19	Global North	Centralized	NA	Info.T.	Y	NM	NM	NM	0
ViruSafe	Global North	Centralized	GPS	Track.T.	Y	NM	NM	NM	1
CovTracer	Global North	NA	GPS	Track.T.	Y	Y	NM	Y	1
Rakning C-19	Global North	Centralized	GPS	Track.T.	NM	Y	N	Y	1
Zostaň Zdravý	Global North	Centralized	GPS	Track.T.	Y	NM	N	NM	3
GH COVID-19 Tracker	Global South	Centralized	GPS	Track.T.	NM	Y	N	NM	2
Coronavirus Algérie	Global South	NA	GPS	Track.T.	NM	NM	Y	NM	10
NICD COVID-19 Case Investigation	Global South	NA	GPS	Track.T.	NM	NM	NM	NM	2
Kenya Covid-19 Tracker	Global South	NA	GPS	Track.T.	NM	NM	Y	NM	1
Coronavirus UY	Global South	Centralized	GPS	Info.T.	NM	Y	NM	Y	1
COVID-19 Provincia de Santa Fe	Global South	NA	GPS	Track.T.	Y	Y	Y	NM	2
Bolivia Segura	Global South	NA	GPS	Info.T.	NM	NM	NM	NM	6
CoronApp-Colombia	Global South	NA	GPS+BL	Track.T.	NM	NM	NM	NM	3
Coronavirus-SUS	Global South	NA	NA	Info.T.	NM	NM	NM	NM	4
Coronavirus Australia	Global North	NA	GPS	Info.T.	Y	Y	Y	NM	6
Canada COVID-19	Global North	Decentralized	GPS	Track.T.	Y	NM	N	NM	0
COVID-19 Tam	Global South	NA	NA	Info.T.	NM	NM	NM	NM	0
BeAware Bahrain	Global South	Centralized	GPS+BL	Track.T.	NM	Y	Y	Y	1
Korona Önlem	Global North	Centralized	GPS	Track.T.	Y	Y	N	NM	0

Y: Yes; N: No; NM: Not Mentioned; DC: Data Collection; DS: Data Sharing;
DP: Data Processing; NM: Data Retention