The Rise and Fall of COVID-19 Contact-Tracing Apps: when NFRs collide with Pandemic

***Abstract*—To complement the manual contact-tracing methods, a flood of coronavirus-related apps was launched in the first half of 2020. Despite the incredible promises made by the governments, contact-tracing apps did not live up to expectations. We analyzed the government commissioned contact-tracing apps from four countries in order to understand the non-functional requirements (NFRs) and socio-technical factors that hindered the success of these apps. We used the user reviews from the app stores for iOS and Android versions, and identified top news articles related to each app. We analyzed the timeline of events through news article along with the app reviews, NFR analysis, cultural comparison, and political influences. Our investigation revealed that the dominant factors behind the negligible success of these apps are complex and entangled with the cultural and political dimensions rather than being just technical. The multilayer diversity of the target users also impacted the design and development of contact-tracing apps in an extremely challenging situation. Our analysis brings into light important elements that are not normally considered as NFR but should be studied in the design of crisis management apps.**

Keywords—COVID-19, Contact-Tracing Apps, Non-Functional Requirements, Public Good, Crisis Management

I. INTRODUCTION

The global pandemic of COVID-19 has presented numerous challenges to manual contact-tracing such as the incubation period, various symptoms and the asymptomatic super spreaders. To complement manual contact-tracing methods, governments around the world began to consider alternative technological solutions to expedite the process, and there was a rush to launch government sponsored or supported coronavirus-related apps in the first half of 2020 [1]. The idea behind the design of a contact-tracing app was to make use of Bluetooth and, in some cases, GPS technologies on mobile phones and provide a low cost, low energy solution for people on the move in order to record community interactions for a period of time related to the period considered to represent the danger of infection transmission.

The use of apps for contact-tracing promised great benefits in terms of instant recording of interaction and mitigation of the limitations and biases of patients' memory, and in theory has been considered a very effective solution for the large scale of the COVID-19 pandemic [2]. The similar concepts of exploiting mobile devices and apps were seen previously during the Ebola virus outbreak in 2014-2016 [3]. Earth Institute at Columbia University launched one of the few Ebola contact-tracing apps which was used for collecting and analysing contact-tracing data in Guinea [4]. It was reported that the app showed potential benefits for improving the quality of the process of data collection and analysis for the health experts to contain the epidemic [5]. However, the case of COVID-19 on the global scale is very different from Ebola.

In 2020, Singapore took the lead in developing a contact-tracing app called *'TraceTogether'* in order to expedite the contact-tracing of COVID-19, and many governments around the world jumped on the bandwagon [6]. This turned out to be a real-time test for the governments of how much their citizens would trust them with surveillance and monitoring of their locations, movement and contact data. As we moved into 2021, several countries have endured the second, and are going through the third wave of COVID-19, whereas some countries never managed to control the first wave properly. With millions of dollars poured into the development and publicity of contact-tracing apps by governments around the world with the promise that these apps could be the 'silver bullet' for battling the spread of COVID-19, but they were not.

COVID-19 contact-tracing apps faced significant challenges when it came to social acceptance in almost all countries. Despite the hopeful promises made by the governments around the world, to our knowledge no contact-tracing app lived up to expectations and the theoretical benefits of these contact-tracing apps have not been realised in practice to full potential anywhere in the world. A number of countries like the United Kingdom and Norway had to pull their respective apps off the stores by mid-2020 after a significant number of issues of performance or privacy were reported. No matter how technologically sound, these apps could not provide successful outcomes without the relevant social factors that require the approval and acceptance of the app users [7].

To understand the social phenomenon behind the ineffectiveness of COVID-19 contact-tracing apps, we analysed the government commissioned contact-tracing apps from four countries, i.e., Australia, Italy, Germany and India. We downloaded the user-reviews from the app stores for their iOS and Android versions using the AppBot[1] platform, and identified top news articles using Factiva[2] to follow the social event-timeline for each app. Our study included the analysis of the timeline of events through news articles, content analysis of the app reviews, Non Functional Requirements (NFR) analysis, cultural comparison, and the study of related political inferences. Our investigation revealed that the factors behind the negligible success of these apps are related not only to both social and technical aspects but also entangled with the specific culture and political system of the country. We also posit that lack of diversity and inclusion in target users on such a large scale during an unprecedented crisis could have hindered the success of the apps. Furthermore, the poor integrated design of the overall socio-cyber-physical system and contact-tracing workflow in which the apps were going to be deployed also led to an extremely modest contribution of the apps to the overarching system goal i.e., prevent virus spread.

Contributions of this study are as follows:

[1] https://app.appbot.co/

[2] https://professional.dowjones.com/factiva/

1. *Analysis of 590, 912 reviews of contact-tracing apps from both Apple and Google app stores starting from the launch of the app till 18th March 2021, complemented with content analysis of news articles about these apps.*
2. *Identification of the complex relationships between relevant NFRs and socio-political-cultural factors in the development of contact-tracing apps*
3. *Multivocal perspective of how and why these relationships should be considered in the design of future crisis management and public apps in general*

The rest of the paper is structured as follows: Section II discusses background and related work. Section III outlines research motivation and Section IV describes research methodology. Section V presents results. Section VI discusses threats to the validity and section VII provides conclusion.

II. Background and Related Work

The concepts of contact-tracing apps as a mean of surveillance and tracking movements of people is not new to COVID-19 pandemic and have been utilized to augment the manual contact-tracing during the Ebola outbreak [8]. A recent study suggested that a carefully designed app could be effective in providing additional support to manual contact-tracing in expediting the process [9]. Singapore became the first country to launch its app *TraceTogether* in March 2020 and Switzerland was the first country to use the Google and Apple's exposure notification system in May 2020 [10]. Different countries adopted different design and modelled the app based on their cultural and ethical requirements, such as centralized, decentralized or hybrid [4] while prioritizing the NFRs such as privacy, transparency, security, trust and reliability, and at the same time attempting to achieve effectiveness and user satisfaction [11].

The global nature of COVID-19 makes it on a much larger scale and more complicated than the Ebola outbreak. During a pandemic or any crisis event, it is people's behaviour towards the uncertainty of the crisis that makes the app technology-based solutions very different from ordinary apps [12]. Since the launch of the contact-tracing apps it has been observed that social aspects of any country such as culture, ethical and legal frameworks around digital technologies, and citizen behaviour outside the usage of app are critical to the adoption of the app and its usage during the pandemic. Unlike other government-sponsored apps, contact-tracing apps needed convincing the citizens of their utility especially for the voluntary mode of usage, and hence there was a need for media and marketing. This brought a new perspective on these apps, and in the countries where there is low trust in the government, the support of the app by the government was taken with scepticism.

Level of trust in the government became somewhat equivalent to the level of trust people showed in sharing their movement data with the governments via contact-tracing apps [2]. In countries like Germany and Switzerland [12] governments had to make extra efforts to gain public trust beyond mere marketing such as voluntary app download, open source code, inclusion of reputable research organizations in development and developers responding to the app reviews of the users. Despite these efforts only around 20% of citizens in Germany and 15% in Switzerland downloaded the app, and the fraction of active users are fewer than that [12]. In Australia, even though it was optional to download the *CovidSafe* app, it was tied to the condition of ending the lockdown imposed since March 2020 [13]. This led to a sense of scepticism in the media and the general population, and the fraction of citizens who downloaded the apps remained much lower than Germany or Switzerland. In Canada to gain the trust of its citizens, the contact-tracing app called *COVID Alert* was open source, required no identifiable information from users, and all data was to be deleted after 14 days. And yet, according to a survey [14] two-thirds of Canadian citizens said they would not download any contact-tracing app, considering it to be invasive to their privacy. A simulation study on Japanese contact-tracing app showed that it required almost 90% of the population to download and actively use the app for the app to be effective [15]. Distrust and lack of effective communication on the benefits of the French contact-tracing app were the top factors for not using the app as reported in a survey conducted with health students [16].

Some of the technical requirements related to socio-economical demographics of the countries were ignored during app design [17]. In Singapore, approximately 20% of the population do not have the adequate technology to even use their contact-tracing app *TraceTogether* [12]. Similar concerns were raised with Irish Heath Service Executive's (HSE) *Contact Tracker app* with respect to the backward compatibility issue, regarding older iPhones, with Apple [18]. The unique nature of the COVID-19 global pandemic has brought new insights on how to elicit and define functional and non-functional requirements for contact-tracing apps from multiple perspectives [19-26]. In our research, we focused on the NFRs as they are tied to the social context and usage of the app that is outside the mobile device and originates from cultural and political landscape of a country.

III. Research Motivation

Technology Adoption Model (TAM) states that the success of any technological solution lies in the "actual use" of technology by the intended users [27]. The actual use here signifies the 'behavioural intention', or in other words the 'attitude' of people towards the technology. It has been observed that the dissatisfaction of users can result in software project failures even if delivered on time, on budget, and with high quality [7].

One of the less explored dimensions of mobile apps and their critical use is during *crisis management* whether it is a natural or a man-made crisis. The nature of every crisis is unique to the use of associated mobile apps by the target users, and the social context of their usage. It is therefore critical to assess the utility and success of such apps from point of view of the users. If the users cannot see the usefulness in the time of crisis, their distrust and disappointment will lead to rejecting it thus causing the failure of the app. More than 50 contact-tracing apps were launched during 2020 [11] around the world and yet all of them faced various challenges when it came to adoption by the target users. Contact-tracing apps required the governments to convince their citizens to install and use them although there was no tangible daily and individual benefit as in common apps (social media, activity or diet tracking, *etc.*), and had to do marketing for the promotion of these apps. The media attention created a complex social dimension around the behaviour of citizens

towards these apps depending on the political landscape and the culture of the country.

The negligible success behind the multimillion dollar contact-tracing apps around the world [26] has made many curious about finding the reasons for users rejection of these apps[28]. This curiosity motivated us to explore the unprecedented social dimensions and selected NFRs that may have hindered the adoption of these apps.

IV. Research Methodology

Our aim in this study was to investigate the contact-tracing apps from NFRs standpoint in the context of cultural and political influences. The importance of a particular NFR could be defined within a specific political culture that we perceived to have formed the behaviours of the citizens on how they approached the app to download, install and use it. Based on Hofstede cultural dimensions, we selected four countries [29] and their government sponsored or supported contact-tracing apps. The selected countries include: very high individualistic and indulgent culture of Australia, the highly pragmatic and long term oriented culture of Germany, the top-down power hierarchy and less individualistic culture of India, and the high individualistic and less indulgent culture of Italy (see Fig. 1). When it comes to the trust index of the citizens of these countries on their governments, India is the only country where people put more trust in their political leaders compared to Australia, Germany and Italy.

Fig. 1. Hofstede cultural comparison of selected countries [29]

In order to understand the social dynamics around the (dis)satisfaction of the users with contact-tracing apps, we used AppBot platform to download and qualitatively and quantitatively analyse 590912 reviews from both Apple and Google app stores starting from the launch of the app till 18th March 2021. We conducted sentiment analysis on the overall reviews for each app using AppBot data. We also identified and qualitatively analysed the reviews around the top discussed topics of NFRs in reviews and media, i.e., Privacy, Trust, Transparency, Effectiveness, Security, Reliability, User Satisfaction and Acceptance [30-32]. We used Factiva to collect the news articles to identify the relevant media coverage of the contact-tracing apps in these countries in order to understand the socio-political event-based timeline around the acceptance or rejection of the apps and the reasons outlined in the news.

Our analysis stems from app reviews, as common in RE, but it is complemented by news articles as we believe that capturing the information loop between recognised media and user opinions is fundamental if one wishes to account for socio-political factors. More in detail, the following reasons motivated us to consider news and not app reviews only:

- *While user reviews include a large number of opinions, these are rarely in-depth analysis, and tend to express the viewpoints of a younger population that commonly use digital products and provide feedback on them.*
- *Newspaper represents expert-based, in-depth analyses that contrast the voice of multiple strata of citizens with the intention of politicians and can influence the opinion of the users themselves.*
- *Newspapers can provide contextual information about the interplay between the app and the current state of the pandemic.*
- *Newspapers can provide information when there is no app review, as, e.g., before app release, to account for rumours and feelings, or when the app is not used anymore, to account for post-mortem reflections.*

In other terms, while app reviews can give an aggregate idea of what is the general feelings about the apps, news article can give an in-depth and broader contextualisation. The data were analysed as follows. One researcher was dedicated to the analysis of each app and was required to produce a textual summary of the analysis. Each researcher had familiarity with the app, its cultural context and the native language, to provide an informed analysis. The other researchers reviewed the analysis in a meeting to reduce bias.

- *For app reviews, we made sentiment analysis and frequency analysis of terms that were related to the topics of interest, namely the NFRs. This can be regarded as a semi-automatic closed coding, where the codes refer to the NFRs. For each specific app, and for each NFR, the subject provided a written summary concerning the content of the app reviews.*
- *For newspapers, the researcher considered the list of articles from Factiva, performed an opportunistic selection based on the titles, and classified their content based on the NFRs. Critical analysis was performed on the newspapers and used to complement the summary based on the reviews.*

In this paper, we report the summaries for each app produced by the researchers, and their complementary review oriented to reduce bias. This contribution shall be regarded as a *perspective paper,* as it expresses the opinion of the researchers involved in the analysis, who are also the authors of the paper. As such, it does not aim to provide an objective view, but to use the phenomena observed to trigger a vision about RE for crisis management apps, and software products oriented to public good in general.

V. Results

Table I. shows the results from AppBot with the overall number of review count for each app in respect to the platform with the average star rating and the percentage of positive sentiment within the reviews.

Country	App name	Average Star Rating (out of 5)		Review Count		% of Positive Sentiment in Reviews	
		Google	iOS	Google	iOS	Google	iOS
Australia	CovidSafe	2.9	3.1	9,819	3,940	32%	29%
Germany	Corona-Warm-App	2.9	2.9	63,848	18,462	28%	23%
India	Aarogya Setu	4.3	2.9	459,457	5,088	87%	34%
Italy	Immuni	2.9	2.8	24,495	5,803	30%	25%

TABLE I. Statistics from app reviews as of 18th March 2021

On Google store, Indian app *Aarogya Setu* has the highest volume of reviews as well as the most positive sentiments expressed by the users in these reviews, however, India never

managed to get over the first wave of the pandemic (see Fig. 2). On a closer look on the Indian app reviews, a significant number (around 25%) were politically motivated, rather than focusing on the app, its functionality or performance.

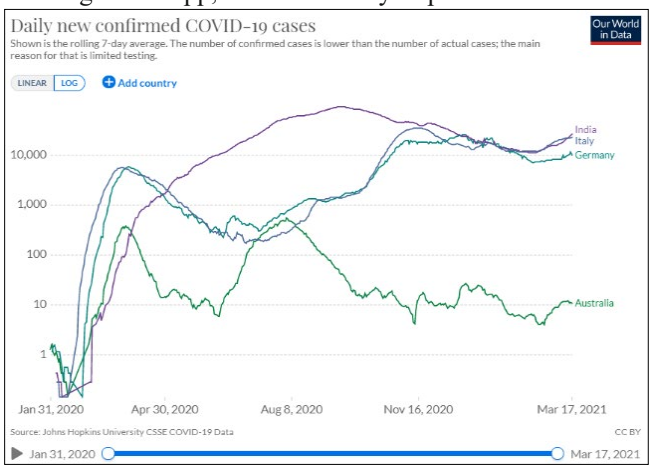

Fig. 2. Statistics of COVID-19 for selected countries [3]

Fig. 2 represent the situation of the spreading of infection of COVID-19 in the selected four countries. Even though Australia managed to control the pandemic with its harshest border control measures and longest lockdown (in the state of Victoria), their *CovidSafe* App was only able to identify 19 unique cases in the whole of 2020. The German *Corona-Warn-App*, and the similar Italian *Immuni* App, are the best among the selected in terms of NFR specially privacy and data protection, yet unable to gain the trust of their citizens as expected and not been very helpful in the struggle to stop or overcome the second wave of COVID-19.

We now present the results of our analysis from AppBot and media articles for each of the *four* countries. We provide extracts from media articles and app reviews under each NFR under each section in text boxes.

A. Australia - CovidSafe App

CovidSafe App was announced on 14th April 2020 by the Australian Government as a digital contact-tracing solution and as a way out of lockdown based on the number of downloads by Australian citizens. The app is designed on the same protocols as Singapore's *TraceTogether* app. The app tracks encounters between users and later allowing a state or territory health authority to warn a user they have come within 1.5 meters with an infected patient for 15 minutes or more. There were immediate concerns regarding privacy of users since the app was launched. The source code of the app was finally released publicly in May 2020 around the time when there was a public hearing in the senate about the effectiveness and privacy implications of the app. The app has cost over 2M AUD out of which 700k AUD were reported to be used for Amazon Web Services. The app was made available on 26th April 2020 to register with Australian phone numbers. Over a million people downloaded the app within 24 hours of its launch and four million by second week. But the state and territory health authorities were not able to access data at that stage. Up to seven million downloads have been reported officially till date for the app, however the active number of users are unknown.

TABLE II. TOPIC ANALYSIS FOR COVIDSAFE IN GOOGLE STORE

Topic	Positive	Negative	Matches	Overall %
Uninstall	2	683	752	7.7
Privacy	52	45	229	2.3
Security	27	48	114	1.2
Trust	5	46	75	0.8
Transparency	3	6	17	0.2
Reliability	1	5	7	0.1

TABLE III. TOPIC ANALYSIS FOR COVIDSAFE IN APPLE STORE

Name	Positive	Negative	Matches	Overall %
Uninstall	0	211	244	6.2
Privacy	24	52	179	4.5
Location	8	79	155	3.9
Security	8	32	58	1.5
Trust	3	26	40	1
Transparency	3	10	14	0.4
Reliability	1	6	9	0.2

1) Privacy

The Australian media gave a lot of attention to the *Privacy* of CovidSafe app and since its launch 1536 articles are published that discussed this topic from various perspectives. This generated great public debate on the topic by the public. Some users in app stores voiced their opinions in regard to the news that the Australian government was not adopting the Google/Apple framework to provide data privacy.

Until the government switch the app to Apple / Google API, I'm refusing to have this on my iPhone. Even the UK government quickly took the steps in the right direction for their citizens.

*Till this app is using centralised data collection that does not respect our **privacy** I won't use this app.. Follow Germany, UK, Canada, and other respected countries and use decentralised data collection using Apple/Google APIs that doesn't give the governments or anyone to track all my movements and is actually working!!*

2) Transparency

The transparency issues related to the CovidSafe app were focused around not adopting the open source model of development and hence no involvement of anyone outside the contractors recruited by the government. Not releasing the code initially gained attention of computing research institutes as there were not in a position to provide public with assurances on effectiveness of the app. The media provided some conflicting statement around the transparency of data and decision-makings of the app.

*Seriously, you need more detail in your release notes. If you've snuck something in that utilises geo-coordinates without telling me, I'm going to be apoplectic in the moments before I uninstall the app. If you want usage, we want **transparency**!*

*Despite how terrible the app is. The lack of **transparency** is atrocious. I can't trust the security of this application if they aren't releasing the source code.*

3) Trust

Trustworthiness of the CovidSafe app became entangled with polarization of political views due to the media and promotions on the app starting from the announcements of the prime minister and then other members of the cabinet. Around $60M budget has been spent on the marketing of the app. 971 media articles have discussed the issue on why we should or shouldn't trust the app, giving rise to the fake news on social media regarding app being used as an espionage tool rather than contact-tracing. In app reviews we can see that not adopting the Google Apple framework also deteriorated the trustworthiness of CovidSafe app in later versions.

*This new version using the flawed herald protocol drains my iPhone 12 Pro Max battery and also requests location (which I've now turned off due to **trust** issues). It's clear that using the exposure notifications framework that*

[3] https://ourworldindata.org/covid-cases

Apple and google made is the best option. Very unfortunate that the herald protocol was chosen.

I reinstalled the app after iOS 13.5 came out thinking it would support the more private exposure logging system Apple & Google developed but it doesn't. Do not install. Government agencies are already abusing warrantless access to our metadata and trying to weaken encryption; I don't think we should ***trust*** *them with more data.*

4) Reliability

Inability to deliver the expected outcomes to the users puts a question on the reliability of the app. With the passage of months, second wave of Covid-19 in the state of Victoria and outbreaks in other states by the end of the year, most of the people who downloaded the app were not active users anymore.

Totally useless because difference in case counts for two people sitting side by side. My wife's phone says 1 covid case within 500 meters, my phone says no positive case within 500 meters. Which one to believe? Not ***reliable*** *because people turn off bluetooth to save battery, especially when travelling.*

Worthless app.. App said I was safe even though I had symptoms and eventually tested positive. Not at all a ***reliable*** *realtime assessing app.*

5) Effectiveness

CovidSafe app was unable to prevent the second wave in the state of Victoria. During the Black Lives Matter march and other events people were strongly recommended to use the app. However, by the end of the year, according to media coverage and app reviews, CovidSafe app did not provide the results it promised. The government did not accept the app was ineffective and by end of the year, there was experiments with changing the app's protocol, this time to VMWare's Herald but not the Google Apple framework that the majority of the reviewers wanted to put their trust on.

It doesn't actually do anything. It has not saved any lives or built a network of infected people to track down. It's ***effectively*** *a pointless existence, plus the contract to build was uncompetitive and ridicules expensive cost to build. $12m?? To some liberal party donor $$... just use the Apple or google tracking app. The USA government already know everything about me.*

6) Security

Though 1750 articles were written in media around the topic of security and CovidSafe app, the concept of security is different to how it is defined as a NFR of the app. Media coverage and user reviews dealt with the topic of security of personal data, creating false sense of security after installing the app, security of the mobile devices etc.

Was fine at the start, though the Herald protocol has caused it to drain around 100x the battery (0.4% to 25%). Samsung SM-G988B/DS on Android 11 with the December ***security*** *patch.*

Extremely unclear as to why It requires GPS to be turned on all the time to work. From a ***security*** *perspective it's unacceptable.*

Please review the 15-minute threshold for logging - I'd want to know if a positive case was near me for 1 minute. It currently feels like false ***security*** *for the sacrifice of battery and bluetooth audio continuity.*

7) User Satisfaction and Acceptance

In terms of the number of reported downloads around 7 million, and the sentiments scores based on the reviews of the users, and the media coverage, CovidSafe has not performed well to achieve user satisfaction and acceptance.

A stuff up by [PM] that cost the taxpayers millions and is yet to provide any real benefit, uninstalled.

B. Germany - Corona-Warn-App

Corona-Warn-App first launched on June 16, 2020 and has been updated several times after the fact. The app has been developed using Google and Apple's Exposure Notification framework and works with Bluetooth low energy, and stores locally the randomized identifiers of the other phones it comes in contact with. The unique identifiers of each phone are valid only for 10-20 minutes and are updated thereafter. Among the global contact-tracing apps split over centralized vs decentralized mode, the German app took the more secure decentralized path. Unique keys, generated several times per hour, are used to identify each smartphone. The keys of close contacts are scanned and stored locally in the device, and only voluntarily shared on a central server, when the users test positive. No personal data is stored by the app. The app was launched in two languages, German and English, and has since been updated to include Turkish, Bulgarian, Polish and Romanian, with plans to include Arabic and Russian.

As per the statistical forecasting by Oxford University's Nuffield Department of Medicine and Alphabet Inc (Google) [33], a contact-tracing app, such as, Corona-Warn-App if regularly used by 15% of the population alongside a well-staffed contact-tracing workforce can potentially lead to a 15% drop in overall infection rates and an approximate 11% drop in COVID-19 deaths. With 25.7 million downloads as of 18th February 2021, more than 20% of the population in Germany has already downloaded the contact-tracing app. While the number of downloads, in proportion to the population, is encouraging to compare with other countries such as Australia, the number is still low. In a country of more than 83 million inhabitants with approximately 57 million of them owning smartphones, the contact-tracing app cannot be simply termed as "success" or the "best" contact-tracing app, as frequently stated by politicians. While the German app, against some odds, seems to have more than 25 million downloads, the number of downloads is still less than half of the maximum number and only a third of them seem to be using it right [34]. The app completed 100 days in operation on September 23rd 2020. The officials reported only 5000 of 277376 people (that tested positive for COVID-19 in Germany) voluntarily shared their result as positive and their contact results on the app. Despite such results, the app was termed as the "best app" [35].

TABLE IV. TOPIC ANALYSIS FOR CORONA-WARN-APP IN GOOGLE STORE

Name	Positive	Negative	Matches	Overall %
Transparency	118	25	247	0.4
Reliability	20	94	143	0.2
Privacy	46	15	96	0.2
Uninstall	0	61	71	0.1
Security	15	9	34	0.1
Trust	1	13	19	0

TABLE V. TOPIC ANALYSIS FOR CORONA-WARN-APP IN APPLE STORE

Name	Positive	Negative	Matches	Overall %
Transparency	89	15	152	0.8
Reliability	4	41	50	0.3
Security	4	1	11	0.1
Uninstall	0	9	10	0.1
Privacy	1	1	9	0
Trust	0	1	3	0

1) Privacy

With the best of privacy provided by the German Corona-Warn-App, the concerns were raised on how useful it would be in a situation of contact-tracing, with the media coverage of 177 articles till date discussing the privacy issue of the app, how much privacy could be ensured in the case of contact-tracing and effectiveness of the app.

Does not work without Google Play services which means that your ***privacy*** *is in the hands off that company*

It must now be a matter of effectively protecting people's life and limb, instead of cheering the data protection fetishists in our country.

*2) **Transparency***

Germany's Corona-Warn-App, vis-à-vis numerous contact-tracing apps from other countries, stood out on several levels. The app development was based on democratic principles, wherein the federal health institute - Robert Koch Institute (RKI) (i) involved reputed public and private partners for developing and supporting this app, such as SAP, Fraunhofer research institute, Deutsche Telekom, and Centre for Information Security, (ii) maintained transparency in the source code management by making it open source from the outset of its launch, and (iii) designing the app based on GDPR principles to alleviate any issues related to data privacy. The app was fully backed by the government as support to the manual contact-tracing system and for spreading awareness in public on coronavirus. Some users took a different view on this transparency [36].

The taxpayers money spent on this was useless. This app needs to work 100% reliable, should be required to enter public areas and gets the result of a test automatically. That would all be possible with privacy in mind, too. Sad that mediocre companies got the task given by poor politicians...

The more transparency clearly outweighs the disadvantages at the expense of privacy if the function is voluntary. The app should give users the opportunity to voluntarily pass on more information via the app in the event of an infection - for example the time of contact.

However, applauded for the efforts of privacy and transparency by many other users

*I've been using the app since day one and I'm very satisfied. I can't quite understand many of the negative reviews. The app has been running for me so far without the slightest problem. It is explained in a very **transparent** and understandable way which data is collected and why. Everything is very clear. I find the contact diary very useful.*

*If you have taken the (sometimes non-existent) apps from other countries - that's really not bad, and pretty **transparent**.*

*3) **Trust***

Germans still do not fully trust the privacy and data protection of the app, and the concerns remain over the period as suggested by a survey conducted by TU München [37]. The survey reflects that around 9% more people (from July 2020 to August 2020) feel that they will not use the app in any case. More than half of the respondents also mentioned that they do not believe that the app can be effective or can have any impact.

*Saps phone battery and does literally nothing. I don't feel the slightest bit safer nor do I **trust** this madness is real. If they're gonna make an application, make a good one, don't waste my taxes on some wasted useless app. My former review was deleted by RKI.*

*don't **trust** this app.. I don't understand what it does in the background. there is no way to test & check if counts BT contact reliably and correctly. a constantly changing risk score would at least indicate that one's environment over time gets more or less dangerous. or info like "the most recent detected infection was X degrees of separation away from you".*

*4) **Reliability***

The reliability of the app was questioned by many users regarding the circumstances in which they needed when they had to get tested for Covid-19.

*The app was once more **reliable**! On March 11th the test was carried out and asked whether I was using the Corona app. On March 12th I scanned the QR code and there is NO test result to date! How can that be? The letter from the laboratory definitely got to me faster via the post!*

*It takes a long time for the app to start. The information displayed has not changed since 2.2.21. I am losing confidence in the app's **reliability**.*

*Had a corona test Tuesday and until Friday the app shows me that there is no result. Called the doctor on Thursday evening and they had the results. Sorry is not **reliable** for me.*

*5) **Effectiveness***

Many users, from the 25 million that downloaded the app, claimed that they would uninstall the app or will discontinue using it. According to the experts, only a third are active users that are using it correctly [34], which is a major blow to the effectiveness, in addition to and not discounting the fact that a large fraction of potential users did not install the app in the first place.

Who else installed the app besides me? I have the feeling this thing is through. Everyone I know claims to have uninstalled the app in the meantime. At least it makes it clear how many active users the app has.

*Too much data protection in the wrong place. There is no widespread acceptance among the population if only every 7th infection is reported via the app. An app that fulfills its purpose would ensure acceptance. Data protection is good, too much data protection can be fatal. Just because data protection fetishists shout the loudest, you shouldn't give in to them; the general public wants an **effective** app. I still use the app.*

*6) **Security***

There were mixed feelings around the topic of how secure the German Corona-Warn-App is, however, like privacy, the security also is in conflict with the usefulness of the app during unique context of pandemic.

*Very **secure**. A friend of mine looked through the source code, it is the most **secure** app the government has ever released.*

*apart from that, in times of data **security** the app cannot be used properly. i dont know the location of the exposure, the date of the exposure and so on. basically, it doesnt help me in moving around more safely*

*7) **User Satisfaction and Acceptance***

In countries like Germany given the low trust in government, the app had slim chances of success and adoption, especially given the exorbitant 68 million Euros estimated cost of the app [38] by the end of 2021. RKI's democratic practices outlined earlier improved these chances. The developers gained and maintained the trust of the users by staying in contact with the users. The developer-user communication contributed significantly to the adoption of the app.

C. Italy – Immuni

TABLE VI. TOPIC ANALYSIS FOR IMMUNI IN GOOGLE STORE

Name	Positive	Negative	Matches	Overall %
Privacy	176	305	1214	5
Security	92	507	987	4
Battery	10	68	120	0.5

TABLE VII. TOPIC ANALYSIS FOR IMMUNI IN APPLE STORE

Name	Positive	Negative	Matches	Overall %
Privacy	96	119	467	8
Security	48	160	339	5.8
Battery	32	138	282	4.9
Location	16	103	200	3.4

Immuni is the official app for contact-tracing of the Italian government. The app is open source (source code is available in GITHub, with extensive documentation, https://github.com/immuni-app/immuni), and has been developed considering privacy and transparency as primary requirements. It follows the decentralized model, similarly to the German app. Whenever a user is tested positive for COVID-19, a healthcare operator authorizes them to publish their status, so that the people who entered in close contact with the case can be notified. Immuni was announced on April 16 2020, and was released on June 15, without any

financial cost for the Italian government. Reviews on the app boosted in this initial period, remained silent until September, and had a new peak in the beginning of October 2020, which also coincided with the start of the second Covid-19 wave in Italy. Between June 2020 and the time of writing (March 2021), after 10M downloads in a population of 30M smartphone users, only 14.000 of them had used the app to notify that they were tested positive. Considering that, in March 2021, 21.000 new positive cases were identified on average each day, the marginality of the app in its contribution to the tracing process is self-evident. In one single day the number of positive cases in the country is higher than the documented positive users from the start of the pandemic.

1) ***Privacy***

This topic was highly discussed before the app was released, and even non-technical newspapers such as Il Sole 24 Ore ("*The Immuni App changes, it will follow the decentralized model*", Apr. 22, 2020), the financial and economic voice of the country, and Il Fatto Quotidiano ("*Coronavirus, Immuni app: all the aspects to be clarified and why the choice of the technology that will be used is crucial for privacy and security"*, Apr. 23, 2020), a political newspaper, discussed issues related to the centralized vs decentralized model and implications for privacy. The public opinion, which was in favour of maximum privacy and was sustained also by academics and experts in an open letter from April 20, 2020, pushed developers towards a decentralized model. After the release, the topic of privacy is still dominant also in the app reviews. Interestingly, the negative ones note that the app takes privacy too much into account and it does not work as it should exactly for this reason. The public opinions influenced the privacy requirements before the release. Then, the requirements appeared to be too stringent to make the app properly work;

"it should track movements without bluetooth, perhaps using only GPS. Privacy should underlie the need for collective health." "Unfortunately, too much privacy makes the app useless" "Our need for privacy (which is violated with all the other apps) forbids us to exploit this app".

2) ***Transparency***

Transparency of the internal mechanism was highly considered by the developers, as it is visible in the well-maintained GitHub repository of the app. However, this accounts solely for the technical transparency viewpoint that can be evaluated only by other developers, who can inspect and assess the code. When the app is downloaded, it fails to convince the user about its behaviour, as it does not give any information about what is actually doing, as highlighted by the following review:

"No feedback, no stats on numbers of contacts both positive or negative, per day with history on the total and calendar time so to possibly enable tracing by the user of the time and place of each contact (to check whether the app is working properly). Not transparent, should enable users to read all data collected so to cross check also privacy respect. Needs improvement."

3) ***Trust***

Opinions about trustworthiness are quite polarized, with extreme viewpoints, although with a tendency towards the positive side. Of course, the majority of those who did not trust the app neither downloaded it, nor reviewed it. Opinions about trust are visible in some reviews from conspiracy theorists who started the installation process and use the early experience as a trigger for their propaganda:

"I installed it, I read the first app start instruction page .... And I uninstalled IMMEDIATELY, going on was a waste of time! OUR PRIVACY NO LONGER EXISTS!!"

Other viewpoints were provided by government opponents:

"Absolutely useless, uninstalled even though I was not against its use. This pseudo app was designed by an approximate and incompetent government and the result could only be something done with the feet."

On the far opposite side, the review of another (non) user, who is instead a government supporter:

I haven't tried yet I've just downloaded but I trust the Italian Premier Minister Conte and the 5 Stars Movement

This last type of pro-government reviews are extremely rare for Immuni. Two reasons may be behind this situation: on the one hand, the connection between the app and the government was not stressed by the government itself, and, on the other hand, government supporters also observed the limits of the app.

4) ***Reliability***

This topic, with reference to battery life and Bluetooth, was highly discussed in the early reviews, with several complaints especially at the beginning. The need to keep the Bluetooth on (although in a mode that does not consume battery), and GPS on (although apparently required solely in some models, and in principle not needed by the app) are indicated as the source of battery drainage. Recent reviews, from Dec. 2020, have a totally different tone:

Minimum battery consumption, even with bluetooth and GPS always active.

Therefore, the problem, which appeared extremely relevant in the first releases, was apparently solved over time.

5) ***Effectiveness***

Effectiveness of the app in tracing contacts, which is its primary goal, is the weakest aspect of Immuni. The app is regarded as not well connected with the rest of the contact-tracing socio-technical ecosystem, and the roles involved in handling the information about positive cases and notifications are not sufficiently trained, leading to delays. This problem of integrating Immuni within the larger context is highlighted by newspapers, as e.g., the Huffington Post in October 2020, where even the Ministry of Health says *"The problem is not the app but the circulation of information"* and the author speaks about *"The jungle of the offline mechanism",* referring to the difficulties of knowing what to do, and who is in charge, after a subject is tested positive and wants to send notifications to the contacts. Normally, an interaction is foreseen between the subject and some health operator in charge of handling the tracing process, but this was often not successful. Reviews in this sense highlight personal experiences:

After so many months, I had the opportunity to check the operation, and it is useless ... THE SYSTEM DOES NOT WORK, PEOPLE MAKE THE SYSTEM! Healthcare workers who do not know how it works, and notifications were received [by my known contacts] after 27 days

The app in itself is a good idea [...] unfortunately there is no infrastructure to make it effective. After a positive swab I did not have the opportunity to send a notification. Even after calling the help center, I did not have any clue on how to contact this phantom health operator that could make the notification possible.

This situation evolved in December 2020, with a toll-free number to notify a positive state. The introduction of this additional means also suggests the insufficiency of the app to guarantee inclusion, and the need for more complementary channels to ensure the success of contact-

tracing. Interestingly this solution was previously suggested also by a user:

> *It would be sufficient to allow the user to make a notification through a phone number. They could verify if the user was associated with a positive test, and they could send the notifications.*

6) Security

Few reviews provide observations about cyber-security, and they are made mostly in relation to privacy preservation aspects, mixing up privacy and security requirements. Somewhat, general problems of security are not considered by the users, but they were considered instead by experts and legislators. An article from Huffington Post highlighted that the weakest security corner for Immuni was the authentication of the health operator who was involved in interacting with the user who was tested positive and needed to notify its status. Italian law today requires strong authentication of healthcare operators---i.e., with a physical card---, but the law was not active yet at the time of release, and security breaches could occur. Furthermore, before the launch of Immuni, a ransomware was diffused that deceived several users.

7) User Satisfaction & Acceptance:

Low user experience was a common complaint, together with the need to voluntarily open the app every day to make it work properly appears to be a strong drawback. The user is not aware if the app is working or not, and it is not aware of what is doing. The following review is enlightening in this sense:

> *The app is dumb.. it does not give any information, ok, that's the privacy, but psychologically some interaction is needed: give the data of positive cases [...] so that usage is encouraged, send a summary of what you can do in yellow and orange zones [different zone colours in Italy indicate different spread of the virus and different norms].. make it ALIVE!!!"*

Another, shorter observation, makes the frustration of the users even more evident:

> *More useless than the r in Marlboro*

D. India - Aarogya Setu

Aarogya Setu is the Indian Government supported contact-tracing and self-assessment app. Aarogya Setu is the most downloaded COVID-19 contact-tracing app in the world with 170 million downloads at the end of 2020 and available in 12 languages. The app works with Bluetooth and GPS, and all the 'contact' logs of the users are stored on the device and automatically uploaded to a server when a user tests positive. The costs for developing and advertising the app have not been revealed by the government, and only price made public was of 41.5 million Indian rupees, spent on publicity between May and July'2020. On 29th April 2020, the federal government made the app mandatory to all its employees [39]. On 21st May 2020, the app was made mandatory for all departing passengers above the age of 14 through Indian Airports [40]. Legal issues were raised regarding the app being used as a government surveillance tool, including the Supreme Court that termed the mandatory usage of app as *"utterly illegal"* [41]. Tables VIII and IX show the topic analysis data for Aarogya Setu app in Google and Apple stores, respectively. The most discussed topic in a negative sense in app reviews is the uninstallation of the app.

> *Totally useless app. I don't know why people should be forced to have it before travelling. I don't know if it is surveillance app or what; but seriously there should be some **transparency** about it too. Also, person should have right not to have this app; because it's not helpful.*

TABLE VIII. TOPIC ANALYSIS FOR AAROGYA SETU IN GOOGLE STORE

Name	Positive	Negative	Matches	Overall %
Security	784	730	1822	0.4
Uninstall	7	1367	1679	0.4
Reliability	264	353	908	0.2
Privacy	44	626	850	0.2
Trust	93	240	406	0.1
Transparency	47	63	173	0

TABLE IX. TOPIC ANALYSIS FOR AAROGYA SETU IN APPLE STORE

Name	Positive	Negative	Matches	Overall %
Uninstall	0	85	96	1.9
Privacy	2	50	61	1.2
Reliability	11	36	52	1
Trust	5	29	37	0.7
Security	6	22	36	0.7
Transparency	6	8	20	0.4

1) Privacy

Privacy of the app was a major concern from the beginning. The app was used for several purposes, including securing passes during lockdowns and vaccinations, and thus interfaced with other systems with users' data accessible to external entities. Two hackers each from India and France were able to hack into the app and bypass security requirements for user's personal information. The French hacker was able to identify the details of the people who were infected at the Prime Minister's Office, the Indian Parliament and the Home Office [42]. The app was launched without much focus on data protection and a sunset clause (to delete data after a certain amount of time), and a clause in the terms and conditions was pointed out by the Economic Times where users provide their consent and "*agrees and acknowledges that the Government of India will not be liable for … any unauthorised access to your information or modification thereof*" [43].

> *Not useful **privacy** concern govt collect data from user location tracking happen to my phone ,zero productivity of this app.*

> *Lots of improvement to be need Personal **privacy** should be at the apex No proper authenticity of person's Health whether he / she would provide correct information or not?*

2) Transparency

The source code of the app was made publicly available after an outcry by IT specialists on hacking incidents in late May 2020. Further issues regarding the transparency of users' data sharing outside the scope of contact-tracing, lack of informed consent, sunset clause, actual developers of the app, and actual costs for developing and advertising the app were raised in Indian courts. The lack of transparency led to users deserting the app and uninstalling it, with download number although high in absolute sense but was already low in terms of the population of the country.

> *Central Information Commission (CIC) issued a show-cause notice over the Ministry's and NIC's reply (…) stating that they do not have any information about the "creation" of the Aarogya Setu application promoted by the government to contain the spread of COVID 19. The CIC termed the response as "preposterous" and issued a show cause notice to the NIC to explain why a penalty not be slapped on it for "prima facie obstruction of information and providing an evasive reply".*

3) Trust

Approximately170 million users trusted the app to download it, although the actual number of active users is unknown. As discussed earlier in the paper, India has a high government trust index, and a large majority of the positive app reviews thanking the government and the prime minister reflected that trust. However, we posit that trust shown in the

user reviews is towards the government or specifically the prime minister and not necessarily the app itself. The others reported that the app cannot be trusted due to lack of transparency, privacy practices, and inaccurate information.

Not an accurate one, kindly don't trust this. You'll need this at certain locations, use it and dispose it off your phone. You never know what can happen with the data if hacked.
One big scam and fraud. Only installed it because I had to for a flight and then de installed it straight away. Don't trust this app.

4) Reliability

The app, similar to other contact-tracing apps had its own fair share of issues related to the reliability. Similar to other apps, the users reported issues with Bluetooth, GPS, battery drainage, and receiving message to activate the app. In addition to these prevalent issues, the app received mixed reviews about the accuracy of location services required for the secondary use case of Aarogya Setu, wherein, the users received information on number of positive cases in the area of certain radius around them.

I tested covid positive but app continues to report I am safe. I tried assessment option to indicate current health but still its same. I am afraid the isn't reliable basis my experience as it would appropriately alerts people who might have come in my contact.
This app serves the purpose it is designed for, that is to "keep us safe ", I was initially a skeptic, but was able to verify some of the alerts which were very accurate, Thank you Team Arogya Setu, Keep up the great work.

5) Effectiveness

The primary function of the app was contact-tracing, which has been lost among the numerous secondary use cases introduced in the app, and thus deemed ineffective for contact-tracing. This is also reflected in the recent user app reviews which predominantly focus on vaccination registration, while some of the contact-tracing apps have been made obsolete.

6) Security

As evident in the discussions around privacy, transparency and trust, security has been a major concern for the Indian app, especially in the initial versions of the app.

Cyber security is not assured in India, so we don't know that how our data is being used by the government
Government sponsored spying and backdoor logging/hacking app

7) User Satisfaction & Awareness

Low user experience and satisfaction was evident in Aarogya Setu app, with users complaining about the blatant inaccuracy of the information shown in the app. One key difference to the other global apps are the multiple use cases of the Aarogya setu app, in addition to contact-tracing, such as, information on number of people who tested positive in a radius of 500 metres around the user's location, availing special passes for leaving establishments during lockdowns, and recently for vaccination registration. The multi-dimensional use cases of the app were confusing for the users, and the app lost track of the original purpose of contact-tracing.

Useless App.... not practical not working..... govt should stop promoting this type of garbage apps... its only drains battery and not giving accurate information.
today it is not showing any covid updates state wise or overall in India. Instead it has a vaccination column. The Covid updates column has vanished and I cant find any list or data of active Covid positive patients, confirmed and recovered patients as it used to be.

VI. Discussion

In general, NFRs for software are much harder to define, understand and translate into the design than functional requirements [31]. The contact-tracing apps present unique challenges for the app designers that stems from the culture and the behaviour of the users. In the following, we discuss relevant aspects that emerged in this regard, and how the lessons learned can be exploited for future crisis management apps and other software products for public good, which we refer to as *public apps* in the following.

Different countries, different NFRs - In different countries we observed different NFRs were the focus of critique. In Australia, the *lack of transparency* in initial stages and the dominance of political marketing played significant role in the *lack of trust* by the Australians in CovidSafe app. In Germany, the *over protection of data privacy rights* and the *ineffectiveness* to stop the spread of infection contributed to the little success of the Corona-Warn-app. The German app became the classic example of conflicting NFRs. Indeed, we observed that technical transparency does not imply transparency of the app behaviour from the point of view of the user. In India, the *poor security and data protection* lead to some of the *loss of interest and trust* in the *Aarogya Setu* App. In Italy, the *ineffectiveness* and *lack of reliability* contributed to the ill fate of *Immuni* app. These differences in terms of critique are surely linked to inherent differences between the apps (transparency was not considered in *CovidSafe*, while was a primary concern for *Corona-Warn* and *Immuni*). On the other hand, a common trait of the different apps was that some NFRs dominated with respect to others and this imbalance led to failure: *Aarogya Setu* App and *CovidSafe* invested in trace reliability, but failed with transparency and privacy; on the contrary, Corona-Warn-app and *Immuni* stressed privacy, and lost track of functional aspects. When developing *public apps*, there is a need to perform trade-off analysis to balance requirements that emerge from public opinion (such as privacy), and requirements of the general public interest (such as health control), so that the former do not impact the latter, and in general, NFRs do not imapct functional ones.

Public apps, public opinion and Politics - Unlike other apps, contact-tracing apps required media coverage that also formed public perception of how they viewed the apps. The vocabulary and understanding of the NFRs in user's comments on social media and reviews in app stores, is more skewed towards how the media represented the apps rather than how the software developers would define and design NFRs. Reviews of public apps can also be a space for political and anti-political propaganda. With the spread of 5G networks conspiracy theories, the attitude towards mobile technology and the apps met with resistance from those who believed in the conspiracy. A significant portion of reviews, especially in India and Australia, were politically motivated rather than a simple issue report or feature request. Feedback from users on some of the NFRs were addressed over time with multiple versions of the contact-tracing apps. User Acceptance of public apps is usually achieved after a real test in the wild. Developers need to decide whether to make the users unhappy after the first few releases, and exploit the negative feedback to improve, or prevent any issues to happen before the next release.

Public apps, their ecosystem and inclusion problems - A public app is only a building block of a socio-technical ecosystem, and one needs to make sure that all actors involved account for the app, and are trained on the process to follow when downloading the app. The success of these apps depends heavily on the significant proportion of the population downloading and keeping the app active while in public spaces. The diversity of the target population is extremely challenging to include in the design of these apps. To include every facet of multiculturalism, age, expertise levels with mobile devices, economical factors to afford smart phones, digital divide, and multilingualism of a country besides the behaviour and the political ethical frameworks around trust, privacy and transparency could be a next to impossible task. However, for the contact-tracing apps, literally everyone matters. A bad decision of one person can set back the good collective work of the whole community during a pandemic. The contact-tracing apps and their designs clearly showed little to no effort to follow the diversity and inclusion factors that would define the target users of any country around the world. Therefore, to be successfully included in the socio-technical ecosystem, public apps need to consider inclusion as primary requirement.

Individual interest versus public interest - Social acceptance of any software is impacted by its perceived usefulness and effectiveness. If there is no real engagement with the users, it is very difficult for the users to determine its usefulness or effectiveness. This in turn hinders social acceptance. An app that serves the public interest gives benefit in the long run. However, to be appreciated, it should consider providing a direct benefit to the users, with additional functions not strictly related to the main app functionality. Otherwise, the risk is that the app remains forgotten in the memory of the mobile, as it happened in the case of Italy and Germany, or even gets deleted---because it is considered not only useless, but in some cases dangerous.

False sense of security - We have observed that the issue of digital security is either not discussed, or it is mentioned in inappropriate terms in the app reviews. While the public is aware and keen to discuss privacy, issues about security do not emerge unless a security breach occurs that makes everyone aware of the limits of a public app in terms of security. Therefore, when developing public apps, security needs to be discussed by experts beforehand with the involvement of legal authorities, and legal aspects on authentication need to be considered. Consultation needs to consider possible breaches on the side of the public operator, and not only on the user side. Users need to be made aware of the presence of ransomware, which can be developed and successfully deployed before a public app is launched, as it happened in Italy.

The adoption of contact-tracing apps has been observed to be extremely low, despite having clear benefits for the citizens in theory [7]. Governments across the globe spent millions of dollars in developing and promoting contact-tracing apps for little or no benefits in return. Meanwhile the situation of the COVID-19 around the world, with exception of Australia since November 2020, is still not under control. People's focus has shifted towards the vaccines which are now the new promise to show a way out of global pandemic. COVID-19 isn't over yet, and the results of vaccinations are yet to be known. Many countries around the world are now facing the second and third waves and the contact-tracing apps seem to be of little help in stopping or slowing down the transmission of virus, even if it was designed using democratic practices. Bringing technological solutions to address a problem will not help if there is little understanding of the bigger picture for humanity where numerous complex interconnected large scale socio-political-cultural factors play their role.

VII. Threats to Validity

In this study we have chosen four countries based on the difference of their cultural and political landscape. The data collection and analysis are contextual to the story of each of these nations and their struggle with COVID-19 and hence may or may not be generalizable to other countries with similar context. We would like to clarify the point here that the definition of NFRs in user comments and media coverage was very abstract and open to interpretations, unlike being very well defined NFRs in requirements engineering research. The authors had to use their judgment and experience in RE research to analyze and map the topics as correctly as possible.

VIII. Conclusion

In this paper we have presented analysis of NFRs of contact-tracing apps in the context of culture and politics of four countries. Our objective was to understand the reasons about little success these apps were showing in the combat again COVID-19 and why they were not helping the manual contact-tracing as promised. We collected the data through news media articles to understand the narrative of government, media and public perception, as well as a large dataset of the app reviews by the users. Each country had their own issues with contact-tracing apps depending on their culture and political system. It's an unknown whether there will be an app in future that can actually help manual contact-tracing. Even designed with best of the current software development practices and sound technology, it's very challenging to design an app that can take into account the interconnected large-scale socio-political-cultural factors of the world outside the mobile to perform its functional tasks. Nevertheless, we argue that this effort and its clear failure should not be in vain. This is the first time that a certain well-defined functionality, namely contact-tracing, was addressed by multiple groups of developers all over the world in a *hackathon in-the-wild*, and as a result a complex interplay between NFRs emerged.

Future public apps shall benefit from the experience, so that certain mistakes are not repeated, and in particular: 1. Trade-off analysis shall be performed between privacy and functionality; 2. Inclusion shall be a primary concern; 3. The overall workflow and ecosystem in which the app is deployed shall be carefully engineered beforehand, and citizens need to be trained; 4. Politics, and its general perception by citizens, should be a boost and not an obstacle: government with significant support from its citizens should leverage it to facilitate app diffusion while countries where trust in government is limited should not link themselves explicitly to the app; 5. An app pursuing a public interest should also provide an individual tangible benefit in the daily routine of citizens that is well understood and used.

REFERENCES

[1] "https://www.technologyreview.com/2020/05/07/1000961/launching-mittr-covid-tracing-tracker/ [Last Access 19th March 2021]."

[2] S. Altmann *et al.*, "Acceptability of app-based contact tracing for COVID-19: Cross-country survey study," *JMIR mHealth and uHealth,* vol. 8, no. 8, p. e19857, 2020.

[3] "https://www.afro.who.int/news/speeding-detection-slow-down-ebola-smartphone-app-game-changer-contact-tracing-hotspots [Last Accessed 19th March 2021]."

[4] J. A. Sacks *et al.*, "Introduction of mobile health tools to support Ebola surveillance and contact tracing in Guinea," *Global Health: Science and Practice,* vol. 3, no. 4, pp. 646-659, 2015.

[5] L. O. Danquah *et al.*, "Use of a mobile application for Ebola contact tracing and monitoring in northern Sierra Leone: a proof-of-concept study," *BMC infectious diseases,* vol. 19, no. 1, pp. 1-12, 2019.

[6] S. Babones, "Countries rolling out coronavirus tracking apps show why they can't work," *Foreign Policy,* vol. 12, 2020.

[7] M. Bano, D. Zowghi, and F. da Rimini, "User involvement in software development: the good, the bad, and the ugly," *IEEE Software,* vol. 35, no. 6, pp. 8-11, 2018.

[8] K. C. Swanson *et al.*, "Contact tracing performance during the Ebola epidemic in Liberia, 2014-2015," *PLoS neglected tropical diseases,* vol. 12, no. 9, p. e0006762, 2018.

[9] L. Ferretti *et al.*, "Quantifying SARS-CoV-2 transmission suggests epidemic control with digital contact tracing," *Science,* vol. 368, no. 6491, 2020.

[10] "https://covid19.apple.com/contacttracing [Last Accessed 19th March 2021]."

[11] V. Garousi, D. Cutting, and M. Felderer, "Mining user reviews of COVID contact-tracing apps: An exploratory analysis of nine European apps," *arXiv preprint arXiv:2012.13589,* 2020.

[12] "https://cyber.harvard.edu/story/2020-08/global-digital-pandemic-responses-some-reflections-four-country-case-studies [Last Accessed 19th March 2021]."

[13] "Prime Minister, Minister for Health, Minister for Government Services and Chief Medical Officer (2020) COVIDSafe: new app to slow the spread of coronavirus. Media Release, 26 April Available at: https://www.pm.gov.au/media/covidsafe-new-app-slow-spread-coronavirus (Last Accessed7 August 2020).".

[14] "https://www.newswire.ca/news-releases/majority-of-canadians-would-sacrifice-personal-privacy-if-it-helped-stop-covid-19-finds-kpmg-in-canada-survey-891920008.html [Last Accessed 19th March 2021]."

[15] I. Nakamoto *et al.*, "A Peer-To-Peer COVID-19 Contact Tracing Mobile App in Japan: Design and Implementation Evaluation," *JMIR Mhealth and Uhealth,* 2020.

[16] I. Montagni, N. Roussel, R. Thiebaut, and C. Tzourio, "The French Covid-19 contact tracing app: usage and opinions by students in the health domain," *medRxiv,* 2020.

[17] "https://gs.statcounter.com/os-market-share/mobile/australia [Last Accessed 19th MArch 2021]."

[18] K. Rekanar *et al.*, "Sentiment analysis of user feedback on the HSE's Covid-19 contact tracing app," *Irish Journal of Medical Science (1971-),* pp. 1-10, 2021.

[19] L. Bradford, M. Aboy, and K. Liddell, "COVID-19 contact tracing apps: a stress test for privacy, the GDPR, and data protection regimes," *Journal of Law and the Biosciences,* vol. 7, no. 1, p. lsaa034, 2020.

[20] L. Baumgärtner *et al.*, "Mind the gap: Security & privacy risks of contact tracing apps," *arXiv preprint arXiv:2006.05914,* 2020.

[21] Q. Zhao, H. Wen, Z. Lin, D. Xuan, and N. Shroff, "On the accuracy of measured proximity of bluetooth-based contact tracing apps," in *International Conference on Security and Privacy in Communication Systems*, 2020: Springer, pp. 49-60.

[22] S. Sharma, G. Singh, R. Sharma, P. Jones, S. Kraus, and Y. K. Dwivedi, "Digital health innovation: exploring adoption of COVID-19 digital contact tracing apps," *IEEE Transactions on Engineering Management,* 2020.

[23] S. Munzert, P. Selb, A. Gohdes, L. F. Stoetzer, and W. Lowe, "Tracking and promoting the usage of a COVID-19 contact tracing app," *Nature Human Behaviour,* vol. 5, no. 2, pp. 247-255, 2021.

[24] R. Vinuesa, A. Theodorou, M. Battaglini, and V. Dignum, "A socio-technical framework for digital contact tracing," *Results in Engineering,* vol. 8, p. 100163, 2020.

[25] A. Lodders and J. M. Paterson, "Scrutinising COVIDSafe: Frameworks for evaluating digital contact tracing technologies," *Alternative Law Journal,* vol. 45, no. 3, pp. 153-161, 2020.

[26] M. Bano, D. Zowghi, and C. Arora, "Requirements, Politics, or Individualism: What Drives the Success of COVID-19 Contact-Tracing Apps?," *IEEE Software,* vol. 38, no. 1, pp. 7-12, 2020.

[27] P. Lai, "The literature review of technology adoption models and theories for the novelty technology," *JISTEM-Journal of Information Systems and Technology Management,* vol. 14, no. 1, pp. 21-38, 2017.

[28] A. T. Y. Chen, & Thio, K., "Exploring the Drivers and Barriers to Uptake for Digital Contact Tracing," *arXiv preprint arXiv:2103.10113.,* 2021.

[29] "https://www.hofstede-insights.com/country-comparison/australia,germany,india,italy/ [Last Accessed 19th March 2021]."

[30] L. M. Cysneiros and J. C. S. do Prado Leite, "Non-functional requirements orienting the development of socially responsible software," in *Enterprise, Business-Process and Information Systems Modeling*: Springer, 2020, pp. 335-342.

[31] L. Chung, B. A. Nixon, E. Yu, and J. Mylopoulos, *Non-functional requirements in software engineering*. Springer Science & Business Media, 2012.

[32] O. Zinovatna and L. M. Cysneiros, "Reusing knowledge on delivering privacy and transparency together," in *2015 IEEE fifth international workshop on requirements patterns (RePa)*, 2015: IEEE, pp. 17-24.

[33] "https://www.reuters.com/article/us-health-coronavirus-contact-tracing/tracing-apps-may-stem-covid-19-spread-even-when-only-a-few-use-them-study-idUSKBN25U2YM?il=0 [Last Accessed 19th March 2021]."

[34] "https://www.dw.com/de/corona-app-zu-viel-datenschutz-oder-zu-wenig/a-55964585 [Last Accessed 19th March 2021]."

[35] "https://www.zdf.de/nachrichten/politik/coronavirus-100-tage-warn-app-100.html [Last Accessed 19th March 2021]."

[36] "https://www.zeit.de/digital/2020-08/corona-warn-app-coronavirus-eindaemmung-karl-lauterbach-henning-tillmann?utm_referrer=https%3A%2F%2Fwww.google.com%2F [Last Accessed 19th March 2021]."

[37] "https://initiatived21.de/app/uploads/2020/09/ergebnisse-befragung-corona-warn-app-egovernment-monitor-2020.pdf [Last Accessed 19th March 2021]."

[38] "https://www.spiegel.de/netzwelt/apps/corona-warn-app-wie-erklaeren-sich-die-gesamtkosten-von-68-millionen-euro-a-56b5abe1-e0a6-4b1c-9177-9066df3d9b14 [Last Accessed 19th MArch 2021]."

[39] "https://www.indiatoday.in/india/story/centre-makes-arogya-setu-app-must-for-all-central-govt-employees-1672415-2020-04-29 [Last Accessed 19th March 2021]."

[40] "https://www.thehindubusinessline.com/economy/logistics/passengers-with-red-status-on-aarogya-setu-app-will-not-be-permitted-to-fly-says-civil-aviation-ministry/article31639310.ece [Last Access 19th March 2021]."

[41] "https://indianexpress.com/article/india/aarogya-setu-app-mandate-illegal-justice-b-n-srikrishna-6405535/ [Last Accessed 19th March 2021]."

[42] "https://www.thequint.com/tech-and-auto/tech-news/aarogya-setu-app-data-security-issue-raised-by-french-hacker-elliot-alderson [Last Accessed 19th MArch 2021]."

[43] "https://tech.economictimes.indiatimes.com/news/mobile/legal-experts-point-out-liability-concerns-with-the-aarogya-setu-app/75561228 [Last Accessed 19th MArch 2021]."