Roll. No. A016	Name: Varun Khadayate
Class B. Tech CsBs	Batch: 1
Date of Experiment: 10-09-2022	Subject: Cryptology

Aim

Study of cryptology in contact tracing application.

Abstract: Contact tracing applications have flooded the marketplace, as governments worldwide have been working to release apps for their citizens. These apps use a variety of protocols to perform contact tracing, resulting in widely differing security and privacy assurances. Governments and users have been left without a standard metric to weigh these protocols and compare their assurances to know which are more private and secure. Although there are many ways to approach a quantitative metric for privacy and security, one natural way is to draw on the methodology usedby the well-known common vulnerability scoring system (CVSS). For privacy, we applied consensus principles for contract tracing as a basis for comparing their relative privacy practices. For security,we performed attack modeling to develop a rubric to compare the security of respective apps. Ouranalysis shows that centralized Bluetooth with added location functionality has low privacy and security, while non-streaming GPS scored high in security and medium in privacy. Based on our methodology, only two apps were given a high ranking of privacy: Canada's Covid Alert and Germany's Corona Warn-App. They both used the Google/Apple Notification Framework as the basis for their design. To achieve comparable privacy, we recommend that future projects follow their examples in the following ways: minimizing the amount of data they collect and holding it forthe shortest possible length of time; only having features necessary for the app's main function; and releasing design details so that users can make informed decisions.

Keywords: contact tracing; security; privacy

1. Introduction

Amid a global pandemic, our digital world naturally has turned to digital solutions for contact tracing. Governments worldwide have seized this approach, releasing apps to perform automated contact tracing. The majority of these apps are not identical, though they may follow the same design model. Research by Amnesty International [1] was done to assess the privacy or security concerns of individual apps. However, there is no specific method to compare these apps to determine the strengths and weaknesses of a design's privacy and security.

This paper proposes a metric to measure and compare digital contact tracing application's security and privacy. This metric will allow experts to inform users and developers of the current risks in using the technology, which aspects need improvement, and which tracing protocols should be used going forward. It also creates a goal-based view for governments and developers to prioritize components when developing their app.

1.1. Contact Tracing

Contact tracing is the process of identifying and informing people that they have been exposed to an individual who tested positive for a virus so that they may take appropriate actions, such as isolating and testing. Traditionally, this was done manually through an interview with a patient about whom they were near during their infectious period. Then,

the individuals at risk could be contacted. There could also be a public announcement of a location where a patient was and the time they were there. Digital contact tracing aims to perform an automated version of these interviews and notifications by collecting information from users and comparing this information to determine someone's risk level.

1.2. Digital Contact Tracing Methods

Contact tracing is limited by the capacity of human memory when performed manually. Technology can fill the gap of human limitations with recall, and notify individuals that the patient does not know. The general idea is to use information that a device, such as a smartphone, can collect (GPS, Bluetooth) to compare users to a list of individuals who have reported testing positive. The mechanics of this can vary, but the result is informing exposed individuals that they need to isolate and get tested.

1.2.1. Bluetooth-Based Contact Tracing Methods

In this approach, an app broadcasts an anonymous identifier over Bluetooth, while at the same time scanning for other devices broadcasting from the app. When two devices detect each other, they exchange identifiers and log them along with other auxiliary information, such as signal strength.

There are two main designs currently in use. For the first, known as the *centralized* system, a user that tests positive for COVID-19 releases the log of who they have been near to the server. The server then finds matches of these IDs in its database and performs a risk assessment. If the logged individual was close enough to the patient for the set exposure period, they are sent an alert [2]. Typically, the COVID-19 exposure requirement is that they were within 2 meters for at least 15 minutes.

In the second, known as the *decentralized* system, the patient sends their own ID values to the server. Every app periodically pulls the list of positive IDs from the server and looks for a match in its contact logs. The app performs the same risk assessment as before if it finds a match and alerts the user accordingly. The most widely used design for such a system is the Google/Apple Exposure Notification (GAEN) protocol [3].

1.2.2. GPS-Based Contact Tracing Methods

In the GPS approach, the app logs the GPS location data of the phone. The data are either streamed to a server (referred to in this paper as *GPS streaming*) or stored locally (referred to in this paper as *GPS logging*). When someone tests positive, places they had been during the infectious period are identified. Then, in the GPS streaming system, other people that were there at the same time are found, using the location data on the server. In the GPS logging system, notification methods include the following: updating a publicly available map, which people can compare to their movements to see if they were in an at-risk location; a broadcast notification, using a national alert system; or other en masse communication methods [4].

1.2.3. Other Contact Tracing Methods

Other digital contact tracing methods exist, such as QR Codes, or heat maps. QR codes can be used either by a user logging the location themselves through scanning a code [5], or someone at a location scanning the user's QR code to verify that they are low risk and allowed entry [6]. Heat maps are typically displayed on a website and inform users if areas they currently are, have been, or plan to go to are at-risk areas [7].

1.3. Dangers of Privacy Loss

Names, phone numbers, and other pieces of information are direct identifiers that reveal a user's identity. However, they are not the only information that can do so. Indirect identifiers are information which, when combined, identify a user. The combination of zip code, date of birth, and gender is unique for 87% of the U.S. populace [8], while GPS data can reveal personal information, such as habits [9] and home addresses [10], from studying

movement patterns. Specific to contact tracing, data about which users are regularly meeting could be used to create a social web of users.

One way to assess privacy loss from revealed information is to assess the size of the anonymity set, or the entropy [11,12]. A simplified conceptualization starts with everyone having a set amount of anonymity and information learned about an individual, which lowers their anonymity based on how many people also have this attribute. Using the probability that the information is true about a random individual, one can calculate how much anonymity has been lost. Though this style of measurement can be useful, it also has shortcomings. Not all information has known and exact probabilities of uniqueness.For example, if an app does not delete metadata, then it is difficult to assess how much privacy has been lost because the exact data and their uniqueness are unknown.

1.4. Research Method

We began by exhaustively examining the contact tracing literature. We identified 55 different apps spanning 5 architectural categories as well as privacy principles articulatedby experts. Security concerns and possible attacks were also identified. While performing this review, we noted two things: the current security analyses focused on the code not the protocol; and, the privacy and security literature reviewed apps individually without aclear method of comparison between the apps being used. In this paper, we aim to fill both of these gaps.

1.4.1. Privacy

Our privacy scoring system uses metrics based on a consensus of principles for private contact tracing articulated by cybersecurity academics. We used observations made in our literature review to create a series of qualitative statements that could be used to rank whether a particular app *met*, *partially met*, or *did not meet* a particular privacy principle. We then determined the rank of each principle for each app, selecting one representative app for the architectural categories: decentralized Bluetooth, centralized Bluetooth (BlueTrace), centralized Bluetooth (ROBERT), centralized Bluetooth + GPS, and GPS logging. We used a scoring of 1 (met), 0.5 (partial), 0 (not met) for each principle to create a score out of 10, as there are 10 principles. From a comparative standpoint, the apps were placed into a ranking of high, medium, or low. The 5 apps' scores were used to create the thresholds for each of the three rankings. Then, this scoring was applied to the other 50 applications.

1.4.2. Security

Our scoring system draws on metrics from the CVSS directly (see Section 2.3.1), but also adds domain-specific metrics identified as relevant based on our review of the literature. Our threat modeling identified an extensive set of possible attack vectors. Although not provably exhaustive, we propose several attack vectors not previously identified in the literature. For each app and each attack vector, we assigned each metric a score out of 10. Since much of the literature has already focused extensively on software implementation vulnerabilities (see, for example, [13–16]), our analysis focuses on attack vectors based on an app's protocol and design specifications.

1.5. Contribution

We propose a contact tracing app scoring system based on consensus privacy principles for contact tracing and a vulnerability scoring system we developed. The rubric for the vulnerability scoring was defined by ourselves with some ideas based on those of the common vulnerability scoring system (CVSS). Attacks against contact tracing systems with either the goal of accessing private information or introducing false information into the system were created by us to score the security of contact tracing systems. We reviewed the state of the art to identify a taxonomy of contact tracing apps. Then, we applied the scoring creation methodology to a representative sample of the contact tracing approaches. Our final analysis shows that centralized Bluetooth with added location functionality has low

privacy and security, while GPS logging scored high in security and medium in privacy. The decentralized Bluetooth method scored high in privacy and medium in security.

2. Methodology

This paper proposes a method to compare and rank the privacy and security of different contact tracing apps. The privacy comparison will look at how well an app meets a set of principles laid out by experts. The security comparison will look at how severe the most severe vulnerability to the system is. First, 55 apps were researched. The table displaying the entire privacy review is in the support document [17]. Of these, 5 apps representing different methods of contact tracing were selected to create the assessment system.

There are arbitrarily many ways to develop a quantitative metric for contact tracing privacy and security. The important part is that the metric reflects the high-level discussion of problems into a condensed format that is easier to interpret. One natural way to approach this is to draw on the methodology used to create the well-known and widely used common vulnerability scoring system (CVSS).

The review began with searching for all the apps deployed or in development around the world whose function was to notify users that they were exposed to COVID-19. A list of tracing apps available on Wikipedia [18] as well as a list of apps that use the GAEN system [19] were used as starting points. To find the information on the app, official government websites, app stores, and newspapers were examined. Of particular interest were privacy policies, FAQs, open-source code, white papers, and any other relevant information. The focus was to determine if the app meets the privacy principles and what its security-relevant behaviors are.

In cases where the English language material was not published, translation was performed by Google Translate. This limitation is due to the authors only being fluent in English. Despite this, every effort was made to ensure that the review was thorough.

2.1. Motivation of Methodology

A widely used method to assess and compare the severity of a computer system vulnerability is the common vulnerability scoring system (CVSS). The CVSS assigns severity scores to vulnerabilities based on a formula, which depends on several metrics. The metrics examine the ease of implementation and impact of an exploit on the system and the users. The equations used by the CVSS were developed by the CVSS Special Interest Group (SIG), who built a lookup table by assigning scores and a severity (low, medium, high, critical) to previously known vulnerabilities. Having defined numeric ranges for each severity level, the SIG then collaborated with Deloitte & Touche LLP to adjust the formula parameters to fit the metric scores to the SIG's proposed severity ratings. Thus, the equations were created through qualitatively ranking known vulnerabilities, then working backward to create a quantitative method that could be applied to future vulnerabilities [20].

The CVSS was not directly used for the scoring of the vulnerabilities in this paper. This is because the CVSS is designed to compare general vulnerabilities and does not consider privacy, which is a large part of the contact tracing discussion. A metric that is more specialized to the unique requirements of contact tracing will provide more actionable information. For the rubric of the security assessment, some metrics are similar to those of the CVSS. Specifically, attack complexity, required privileges, scope, confidentiality, and the division of the rubric into exploitability metrics and impact metrics are taken and adjusted for contact tracing from the CVSS.

2.2. Methodology of the Privacy Review

The process of the privacy review is laid out in Section 1.4. The specifics of the privacy principles used and the criteria for defining how well an app meets the requirement of a principle are laid out here in this section.

2.2.1. Privacy Principles of Contact Tracing

We chose to adopt the privacy principles articulated in an open letter widely signed by cyber-security researchers [21]. Other statements exist and are similar [22–24]; we chose to use these, as they are signed by a large group of privacy researchers. The 10 principles are as follows:

- **Independent expert review** : the app should be reviewed by privacy and security experts prior to deployment.
- **Simple design**: the average user should be able to understand how the app performs its functions.
- **Minimal functionality**: the app should only perform contact tracing.
- **Data minimization**: the app should collect as little data as possible to function.
- **Trusted data governance**: who controls, has access to, and how the data are used should be known and subject to public review.
- **Cyber security**: best practices should be used for data storage and transmission throughout the system.
- **Minimum data retention**: collected data should only be stored for the infectious period of the individual, according to the WHO.
- **Protection of derived data and meta-data**: these data types should be deleted as soon as they are created in the system, as they are not required for contact tracing.
- **Proper disclosure and consent**: users should be provided easy to understand information on the functions of the app and all data it uses and stores. Users must consent to all data collection.
- **Provision to sunset**: there should be a timeline in place for when the app will not longer be used and all data will be deleted.

2.2.2. Criteria for Privacy Principles

Based on the principles articulated in Section 2.2.1, we propose a set of criteria for defining how well a particular system upholds each principle. Table 1 contains what constitutes a *fully met*, *not met*, or *partially met* for each principle. To keep the assessment in line with the disclosure principle, an app with no information about a principle is treated as not meeting that principle. If the public cannot learn the information about the app's system the public has to assume that the principle is not being met.

2.3. Methodology of the Vulnerability Analysis

A series of potential vulnerabilities were theoretically applied to the systems of the 5 apps. Their ability to prevent or mitigate the attack determined a score based on a predetermined rubric. The score, in this case, is higher the more severe that the vulnerability is to the system. Then, the apps were assigned, based on their security, a grouping of high, medium, or low. These groupings were then used to determine how to apply the scores from the rubric to place future applications into rankings. The process used for this review is laid out in Section 1.4.

The review makes the following assumptions. First, unless there is compelling evidence to suggest otherwise, it is assumed that the information that the authority has provided about the app is accurate as to how it was implemented. This review does not assess whether there are vulnerabilities caused by human error in the implementation. Second, if something is not stated in the documentation, then it is assumed to not be happening in the system. For example, if there is no information about the system using HTTPS when transporting data, the assumption is that it is not.

The actual implementation of an exploit against the system is beyond the scope of this paper. The app systems were not attacked in any way to perform this assessment. The review looks only at the protocol to determine if there is a theoretical vulnerability.

Table 1. Proposed app privacy rubric.

Metric (Privacy Principle)	Met	Not Met	Partially Met
Independent Expert Review	Reviewed prior to release	No formal review process or public documentation	No formal review process but documentation made public
Simple Design	Protocol or design is public	No documentation of design	Some design information
Minimal Functionality	Only contact tracing	Function outside of contact tracing	Related functions require no extra data
Data Minimization	No personal data collected	Detailed health, personal, GPS data	Minimal extra data not for identifying purposes
Trusted Data Governance	Only trusted public entity has access, data stored in country	No stated ownership or outside entity can access	Ownership known, unknown if outside entities have access
Cyber Security	Encryption best practices, audits	Unknown or not best practice	Statements indicating security is used
Minimum Data Retention	WHO 14 day infectious period	Unknown or over years	Longer than infectious period, less than a year
Protection of Derived Data and Meta-Data	Data never created or deleted	Unknown or given to third party	Some data stated to be deleted
Proper Disclosure and Consent	Voluntary use, data release. App can be paused or deleted, available privacy policy	Mandatory use, data release. No privacy policy	Privacy policy unclear or missing expected information
Provision to sunset	Clearly stated when and how to sunset	Unknown or implied to never sunset	Stated but without definite time

When researching applications, we observed that some had bug bounty programs.In some of these programs, such as that of India [25], they would not consider vulnerabilities where the attacker's device needed to be rooted to operate the exploit. However, there is a difference between an attacker gaining root access on a remote system and on a device that they own. Since an app is downloaded onto a device that the attacker controls, root access is much easier to achieve and more difficult to detect and prevent. In this review, if the phone needs to be rooted, it is still considered a valid attack. The access score will, however, be low.

2.3.1. Vulnerability Rubric

Table 2 lists the rubric created for assessing a vulnerability. The rubric contains eight metrics: four exploitability, and four impact. Each metric is scored between 0 and 10, with 10 being the worst-case scenario for that metric, while 0 being the best case. Generally, the scores given are 0, 1, 4, 7, 10, corresponding, respectively, to the ideal best-case, practical best-case, medium-case, bad-case, and worst-case scenarios. The 0 and 1 values were chosen to capture the distinction between perfectly secure and practically secure. In this rubric, something impossible is scored as 0, while something practically impossible would score a 1. Then, the rest of the numbers are evenly distributed up to 10. The metrics are detailed in the list below.

1. **Exploitability metrics**: these are made up of characteristics of the vulnerable component and the attack against it.
   - (a) **Access**: level of access (privilege) to the system required to perform the exploit.
   - (b) **Knowledge**: level of knowledge required to implement the exploit.
   - (c) **Complexity**: what the technical requirements of the exploit are, the computing power, and the workers required.
     - i. **Technology**: the computing power required to perform or create the exploit.
     - ii. **Build**: the amount of workers it would take to build this attack and the time frame they could build it within.
   - (d) **Effort**: how much work it would take to operate the exploit.

i. **Planning**: the amount of components that have to work together to perform the exploit (that cannot just be automated to perfectly work).
ii. **Human**: the number of people required to work together to perform the exploit and whether they are aware of their involvement.

2. **Impact metrics**: these focus on the outcome that an exploit of the vulnerability could achieve.
   (a) **Scope**: the amount of the user base that this exploit could affect.
   (b) **Impact**: severity of what the exploit allows an attacker to do. This can be getting data logs, inputting their own data, etc.
      i. **Data**: the kind of data that an attacker could get access to and how immediately useful they are to them, or how far into the system they are able to place false data.
      ii. **Trust**: how this exploit being implemented will impact the user base's willingness to use the system, or a similar system in the future.
   (c) **Detection**: how easy it would be for someone to realize that this exploit has been used on the system.
   (d) **Repairability**: how easy it would be to fix what the attacker did.
      i. **System**: level of effort required to return system to a state of safely operating again as it was before the attack.
      ii. **User**: how the exploit would affet the individuals impacted by this attack in the long run.

The overall score for a vulnerability will be determined from the values of the rubric metrics. A 0 for any of the exploitability metrics will result in a 0 score for the entire vulnerability. This reflects the idea that if a vulnerability cannot be exploited, it is not a true threat to the system. If none of the exploitability metrics are given a score of 0, then the scores of all the metrics are averaged. First, the metrics split into two parts are averaged to have a single score for that metric, and then all of the metrics are averaged together.The average is chosen as a simple way to compare the different vulnerabilities. The method for calculating the score is given in Equation (5).

$$Complexity = (Technology + Build)/2 \tag{1}$$

$$Effort = (Planning + Human)/2 \tag{2}$$

$$Impact = (Data + Trust)/2 \tag{3}$$

$$Repairability = (System + User)/2 \tag{4}$$

$$Score = \begin{cases} 0 & if\ A \wedge K \wedge T \wedge B \wedge P \wedge H = 0 \\ \frac{A+K+C+E+S+I+D+R}{8} & else \end{cases} \tag{5}$$

where $A = Access$, $K = Knowledge$, $C = Complexity$, $T = Technology$, $B = Build$, $E = Effort$, $P = Planning$, $H = Human$, $S = Scope$, $I = Impact$, $D = Detection$, $R = Repairability$, and $\wedge$ = logical AND.

2.3.2. Attack Tree for Assessing Contact Tracing Application Vulnerability

The attack tree in Figure 1 lays out possible vulnerabilities of contact tracing systems. There are two likely motives that someone attacking a government system designed to protect the populace might have: gain information or break trust. These motives are represented in the attack tree as the goals. Either the attack breaks the privacy promises of the system, or the attack introduces false information into the system.

The arrows in Figure 1 represent the direction that the attack paths flow. The tree lays out 17 different avenues of attack. However, 18 attacks are posed against the chosen five systems. For attack 4, it is pertinent to differentiate the attack between whether an individual or a larger body performed it. Thus, there is an attack 4 and an attack 4.5.

Table 2. Proposed app protocol vulnerability rubric.

Metric	Score 0	1	4	7	10
Access	Prevented at any privilege level	High level of access required, need root access	Medium level of access required, need higher access than regular user but not full root access	Some level of access required, need access beyond the user interfaces	Lowest level of access required, regular users could do this without higher privilege
Knowledge	Full knowledge of the system does not give someone the tools to attack it	Expert level of knowledge required, expert in the field with many years of experience in a specific subject	Advanced level of knowledge required, individual with career in the field	Intermediate level of knowledge required, graduate level student	Novice or fundamental level of knowledge, undergraduate level student
Complexity	Not possible with modern computing power	Highly complex and resource intensive, this requires a large amount of computing power	Medium complexity, requires high end computers	Low complexity, requires an average consumer computer and some tools need to be created	No complexity, this can be performed with minimal computing power, directly on a phone, with a single-board computer, etc.
	Not reasonably possible for any group to design	Large group actor would be required	Multiple people could create with a month of time invested	Single person could create with a month of time invested	Single person could create in less than a month
Effort	Extremely high effort, many components with very specific timing that cannot be automated	High effort lots of components that need to all work perfectly	Medium level of effort, several components required	Low effort, a couple of components required	Very low effort, minimal components or steps
	Would requires a large percentage of the user population to work together	Many people required to help (wittingly or unwittingly)	Multiple people required to help (wittingly or unwittingly)	One or two people working together	One person can perform alone
Scope	Does not affect anything in the system	Affects a single person, Attacker can gain information for one person that they may know	Affects a small group, attacker could target everyone they know	Affects a large group; attacker could target an entire section of the user base or a demographic	Could affect everyone in the system
Impact	Attacker gains no access to alter or view the system	Attacker gains access to de-identified data that are not practically re-identifiable or introduces false data on the device	Attacker gains access to de-identified data that could with effort be re-identified or introduces false data on the server that will be deleted	Attacker gains access to data that with minimal effort can be re-identified or introduces false data that is persistent in the system	Attacker gains access to personal information and identities or introduces false data that are persistent and indistinguishable from real data
	Attack has no effect on the trust in the system	Temporarily lowers trust in the system	Lowers trust in the system	Damages trust in the system	Destroys trust in the system
Detection	Is actively monitored for and prevented	Is monitored for and would be noticed on a daily report	Could take up to a week to recognize	Could take a month or more before it is recognized that the attack was implemented	It is possible and likely that the attack would not be noticed until the attackers revealed their actions publicly (releasing a dataset, making public claims)
Repairability	The attacker did nothing to the system that requires action	Requires minor code fixes to prevent future attacks	Requires alterations to the system and/or removal of the attackers code	The system requires significant alteration/repair	The system requires significant code updates and/or changes in the underlying protocol
	The attacker did nothing to individuals that requires action	The users are affected but no action is required	Some users will have to perform a one-time action to mitigate the effect	The attacker gained access to user information that cannot be altered easily	The repercussions from this attack will affect people on a continual basis and are difficult to quantify

3. Results

3.1. Selected Applications

The five apps chosen as representatives are Canada's Covid Alert, Singapore's Trace-together, Iceland's Rakning C-19, India's Aarogya Setu, and France's TousAntiCovid. Canada's Covid Alert is a decentralized Bluetooth system implemented using the GAEN framework [26]. Singapore's TraceTogether is a centralized Bluetooth system following the BlueTrace protocol [2]. Iceland's Rakning C-19 is a logged GPS system [27]. India's Aarogya Setu is a Bluetooth centralized system that has added GPS streaming functionalities [28]. France's TousAntiCovid is a centralized Bluetooth system that follows the ROBERT protocol [29].

Singapore, India, and France all use a Bluetooth centralized system and were chosen to represent the differences in protocols and behaviors between the centralized Bluetooth apps. The majority of the decentralized Bluetooth apps used the GAEN protocol and were very similar in design. The Canadian app was chosen, as there is a significant amount of information released about it. Iceland's Rakning C-19 app was chosen to represent GPS systems because they released information about the design through source code available online [30].

3.2. Privacy Review

The five apps were reviewed for privacy based on the information made available through released documentation. Table 3 shows the breakdown of whether each of the five apps met, did not meet, or partially met each principle, based on the requirements for each criterion we laid out in Table 1. Then, they were placed in initial rankings as explained in the following analysis.

Table 3. Contact tracing application's privacy principle breakdown of representative apps.

Country	App	Ind.Review	Design	Min.Func.	Data Min.	Data Gov.	Security	Retention	Meta-data	Disclosure	Sunset
CAN	Covid Alert	•	•	•	•	◑	•	•	◑	•	◑
FRA	TousAntiCovid	◑	•	•	Q	Q	◑	•	◑	◑	◑
ISL	Rakning C-19	◑	•	•	Q	•	•	•	Q	•	Q
IND	Aarogya Setu	•	•	Q	Q	Q	•	◑	Q	Q	◑
SGP	TraceTogether	◑	•	•	Q	◑	◑	◑	Q	•	◑

• = met, ◑ = partially met, Q = not met

Canada's Covid Alert released information to users in the form of clear privacy statements, reviews, source-code and FAQs [26,31]. All of the principles are addressed, though they were not all met. It was built using the GAEN API, and the Office of the Privacy Commissioner of Canada performed a privacy assessment [32]. The server is located within the country; however, the data ownership is unknown. It collects very little data about the user and does not ask for identities or identifying information. For the sunset requirement, there is no defined time. It is stated to be when a health authority declares the pandemic over [32]. The Covid Alert was grouped as High.

France's TousAntiCovid is Bluetooth and based on their ROBERT protocol [29]. Though they released the source code for the entire system, there is no mention of a review performed before the release of the app [33]. The governance principle is not met, and it is unclear what personal information the app requests from the user to determine if they minimized data. The server's location is unknown, and there are no assurances of data access limitations or oversight. Data are encrypted on the device; however, it is unknown if they are transmitted securely. The app claims to meet the relevant country privacy laws without specifying how it meets each law or which laws are considered relevant. A privacy

policy available online was not found. For the sunset requirement, there was no defined time limit. It is stated to be when a health authority declares the pandemic over [34]. Since it partially meets more principles than it completely meets, TousAntiCovid was grouped as Medium.

Iceland's Rakning C-19 meets quite a few of the principles and does not meet three of them. A consideration made in the review is that GPS data are highly personal information, and removing someone's identity from them is difficult. The source code for the app is available but not the server side, and there was no mention of a review performed before the release of the app [30]. They state that the GPS data are held for 14 days and that they collect the user's phone number [27]. A national ID number is requested if a positive test result is input. No information was found about how they treat meta-data or what plans there are to sunset the app. Rakning C-19 was given a Low/Medium ranking, meaning either the Low or Medium group would be accepted when the thresholds are determined.

India's Aarogya Setu only met three of the principles. This app is a Bluetooth system, but it also takes some location data from the user and displays that to other users, showing them how many at-risk people they were near [35]. The system does not ask for additional consent to upload information. Once the app is downloaded, if a user tests positive, their account on the server is flagged, and the next time their device connects to the server, it uploads the information requested [28]. There was no whitepaper released about the protocol that they use for Bluetooth or GPS. The information requested includes phone number, name, gender, age, profession, travel history for last 30 days, willingness to volunteer in times of need, and other information [35], which is more than what is required for contact tracing. Nothing is stated about the data governance or meta-data treatment. The data retention limit is longer [35] than the WHO infectious period. The government previously made the app mandatory for anyone employed [36]. For the sunset requirement, there was no defined time limit. It is stated to be when a health authority declares the pandemic over [37]. Due to these factors, the Aarogya Setu app was grouped as Low.

Singapore's TraceTogether does not address all of the principles. The open-source code for a template implementation of their Bluetrace protocol was released [38] but not the code of the specific TraceTogether app. Though four independent experts were consulted to review the security of their token devices [39], there is no mention of the same assessment for the app. The app requests personal information that is not required for the operation of their contact tracing protocol, such as national ID and phone number. The data are controlled by a government authority, though the location of the server is unknown. Data are encrypted on the device. However, it is unknown whether they are transmitted securely. The data retention limit is longer [40] than the WHO infectious period of 14 days. There is no available information about meta-data treatment. For the sunset requirement, there was no defined time limit. It is stated to be when a health authority declares the pandemic over [40]. TraceTogether was grouped as Medium.

3.2.1. Privacy Metric

For scoring the apps, each principle was graded out of 1. Meeting the principle is 1/1, partially meeting is 0.5/1, and not meeting is 0/1. The privacy score of an app is out of a total of 10. The scoring of each app can be seen in Table 4. If one were to attempt to form an internal or weighted ranking of the principles, an argument could be made for any one of them to be more important. Thus, a ranking method that assumes each principle is equally important was chosen.

The ranges for the groups were created by dividing the scale and using the initial rankings of the apps to determine thresholds. Low is 0–4.5, medium is 5–7.5, and high is 8–10. Table 5 contains the numerical ranges for the app privacy rankings.

Table 4. Privacy review of 55 contact tracing apps; breakdown of principle scoring, their final scores and resulting ranking.

Country	App Name	Meets Privacy Requirements				
		Yes	Partial	No	Score	Rank
Australia	COVIDSafe	4	6	0	7	Medium
Austria	Stopp Corona	3	4	3	5	Medium
Azerbaijan	e-Tabib	0	1	9	0.5	Low
Bahrain	BeAware Bahrain	0	0	10	0	Low
Bangladesh	Corona Tracer BD	1	4	5	3	Low
Canada	Covid Alert	7	3	0	8.5	High
China	Health Code	2	0	8	2	Low
Colombia	CoronApp	0	5	5	2.5	Low
Czech Republic	eRouška (eFacemask)	4	4	2	6	Medium
Denmark	Smittestop	4	3	3	5.5	Medium
Ecuador	ASI (SO)	1	5	4	3.5	Low
Fiji	careFIJI	4	2	4	5	Medium
Finland	Koronavilkku	3	4	3	5	Medium
Germany	Corona-Warn-App	7	2	1	8	High
Ghana	GH Covid-19 Tracker App	0	1	9	0.5	Low
Gibraltar	Beat Covid Gibraltar	2	0	8	2	Low
Guatemala	Alerta Guate	0	0	10	0	Low
Hungary	VirusRadar	2	2	6	3	Low
Iceland	Rakning C-19	6	1	3	6.5	Medium
India	Aarogya Setu	3	2	5	4	Low
Ireland	COVID Tracker	5	4	1	7	Medium
Israel	HaMagen	3	3	4	4.5	Low
Italy	Immuni	5	3	2	6.5	Medium
Japan	COVID-19 Contact Confirming Application	6	2	2	7	Medium
Jordan	AMAN APP—Jordan	3	2	5	4	Low
Kasakhstan	eGovbizbirgemiz mobile app	4	2	4	5	Medium
Kuwait	Shlonik	0	1	0	0.5	Low
Latvia	Apturi Covid	4	2	4	5	Medium
Malaysia	MyTrace	1	5	4	3.5	Low
Netherlands	CoronaMelder	5	3	2	6.5	Medium
New Zealand	NZ COVID Tracer	2	5	3	4.5	Low
North Macedonia	Stop Korona!	3	1	6	3.5	Low
Northern Ireland	StopCOVID NI	5	4	1	7	Medium
Norway	Smittestopp	1	2	7	2	Low
Poland	ProteGO Safe	3	4	3	5	Medium
Portugal	STAYAWAY COVID	4	4	2	6	Medium
Qatar	Ehteraz App	0	0	10	0	Low
Russia (Moscow)	Social Monitoring Service	0	2	8	1	Low
Russia	Contact Tracer	1	0	9	1	Low
Saudia Arabia	Tabaud	3	3	4	4.5	Low
Scotland	Protect Scotland	5	3	2	6.5	Medium
Singapore	TraceTogether	3	5	2	5.5	Medium
Slovenia	#OstaniZdrav	6	1	3	6.5	Medium
South Africa	COVID Alert South Africa	4	2	4	5	Medium
Spain	Radar COVID	6	2	2	7	Medium
Switzerland	SwissCovid App	6	2	2	7	Medium
United Kingdom	NHS COVID-19	3	3	4	4.5	Low
United States	CoEpi	1	3	6	2.5	Low
United States	CovidSafe/CommonCircle Exposures	3	3	4	4.5	Low
United States (Ariz.)	Covid Watch	3	3	4	4.5	Low
United States (Calif.)	California COVID Notify	5	0	5	5	Medium
United States (N.Dak. and Wyo.)	Care19 Alert	3	2	5	4	Low

Table 5. Contact tracing application privacy scoring ranges.

Ranking	Privacy Score
High	8–10
Medium	5–7.5
Low	0–4.5

3.2.2. Full Privacy Review

The entirety of the 55 apps researched were judged based on the privacy criteria and given a score. The full analysis can be seen in the support document available [17]. Table 4 displays each app, how many criteria they met, partially met, and did not meet, and their final score and grouping.

3.3. Analysis of the Vulnerability of Contact Tracing Applications

Each attack was theorized against what was known about the five representative apps and a score was determined based on how vulnerable the app was to the attack. A high score is a severe vulnerability. An example of the work done can be found in Appendix A. Due to the length of the full analysis, it is not within this document. The entire analysis of each attack against each app can be found in the support document [17]. Unlike the privacy score, the security review was not performed for all 55 researched apps, as the vulnerability review process is far more involved and requires significantly more time.

3.3.1. Vulnerability Review

The ranking corresponds to how serious a vulnerability in the system is. High indicates that there is nothing of serious concern. Medium means that there are some areas of concern in the security of the system. Low indicates that critical security flaws are present in the system. The apps were given the following initial rankings.

- Canada Covid Alert—Medium.
- France TousAntiCovid—Medium.
- Iceland Rakning C-19—High.
- India Aarogya Setu—Low.
- Singapore TraceTogether—Medium.

Canada's Covid Alert application is ranked as medium because while many of the proposed vulnerabilities have the potential to be exploited within the system, the highest has a totaled average of 7.3. This vulnerability is concerning but not a critical issue with the system.

France's TousAntiCovid application is ranked as medium because while many of the proposed vulnerabilities have the potential to be exploited within the system, the highest has a totaled average of 7.06. This vulnerability is concerning but not necessarily a critical issue with the system.

Iceland's Rakning C-19 application is ranked as high because of the lack of vulnerability. When the attack tree was held against the system of the Rakning C-19 application, none of the proposed vulnerabilities were a viable option against the system, due to the nature of GPS logging. The system is secure against these attacks.

India's Aarogya Setu application is ranked as low because of the nature of the vulnerabilities found. When the attack tree was held against the system of the Aarogya Setu application two of the vulnerabilities received a totaled average of higher than 8. The functionalities within the system leave opportunities for attackers to take advantageand maliciously target users. Allowing the users to see how many individuals are near them currently, or that have been near them, have symptoms or have tested positive forthe virus is a dangerous amount of information to be publishing.

Singapore's TraceTogether application is ranked as medium because, similar to the Covid Alert app, while there are vulnerabilities that have the potential to be exploited and two with average totals of 7, these are only concerning. The application has some areas of concern, though there is no critical vulnerability in the system.

3.3.2. Vulnerability Ranking

Limitations in our methods need to be considered to determine how to score the security. Though the attack tree is thorough, it cannot be proven to be comprehensive. Thus, we chose to look at the most severe vulnerability of the protocol. This way, if a critical vulnerability is found, the ranking of an app will change to low, regardless of other vulnerabilities in the system.

The ranking thresholds were determined from the placement of the apps in the initial ranking and are High 0–3.9, Medium 4–7.9, and Low 8–10. Due to the averaging of the rubric, this ranking method requires that a vulnerability has high scores in many of the rubric categories to be considered severe. Table 6 contains the numerical ranges for the app security rankings.

Table 6. Contact tracing application security scoring ranges.

Ranking	Highest Severity of a Vulnerability
High	0–3.9
Medium	4–7.9
Low	8–10

3.4. Privacy and Security Rankings

A summary of the final scores for the privacy and vulnerability reviews of the five selected applications is in Table 7.

Table 7. Security and privacy scores of the 5 representative contact tracing applications.

Ranking	Privacy Score	Vulnerability Score
Covid Alert	8.5	7.313
TousAntiCovid	5.5	7.063
Rakning C-19	6.5	0
Aarogya Setu	4	8.375
TraceTogether	5.5	7.375

4. Discussion and Conclusions

Contact tracing has entered into the public consciousness due to the circumstances of a pandemic. Though it will slowly fade out of the public eye, such as disinfection procedures and personal protective equipment, contact tracing is a tool of modern medicine. In future viral outbreaks, contact tracing will be used to prevent a pandemic, and whether it is usedin a town, entire country, or globally, it needs to be private and secure. In this paper, we have created an objective metric of how secure and private contact tracing apps are when compared to each other.

From the results of this study, the Canadian Covid Alert app and the German Corona-Warn-App were the only apps to be placed in the ranking of high for privacy. The reason for their high ranking is summarized in a few commonalities found in the choices their design teams made, listed here.

- **GAEN framework**: both apps use the Google Apple Exposure Notification Frame- work, which uses decentralized Bluetooth as the base of their design.
- **Minimalism**: although the German app does allow the user to scan a QR code they were given to see the results of a COVID-19 test, both apps otherwise contain no added functionality, collect almost no information about the user, and any data they do hold or send are deleted within 14 days.
- **Transparency**: both released the source code for their apps, and Canada also sought out experts to perform a review prior to release. Both have comprehensive privacy statements and policies that clarify all the relevant information.

Although our rubric identifies the GAEN framework to be a privacy boon, it is imperfect. It encourages open-source app and server code by providing open-source templates; however, the code of the framework itself is closed. This code is at the OS level, which most companies do not release to the public. The Bluetooth and cryptography specifications [41] are available, but anyone wishing to compare specification to the code cannot do so without Google and Apple's invitation. This leaves users trusting that these companies are acting according to their official statements, and are not collecting or storing data. While code is one way to prevent data leakage, data governance and policy play their part as well and this is considered in the privacy rubric.

The app with the best security of the five was the Icelandic Rakning C-19. The reason for this is that the GPS logging system requires no communication between devices. The only time the app communicates with anything external is when sending the GPS data to the contact tracer, leaving few attack vectors. At the same time, the amount of human

intervention required to analyze the GPS data and verify a positive case makes it the least automated of the systems. Therefore, it is the least viable for larger countries to implement.

This paper is the first to create an assessment method for the security and privacy of digital contact tracing applications. Other research focused on the security of single apps [1,13,14], or performed a review of the security or privacy without creating a metric of comparison [42,43]. That work can highlight security risks in apps. However, a comparison of the apps can provide actionable information to the people expected to use or develop these apps. This overview of the field can clarify what can be done during app development to mitigate privacy and security threats prior to release.

Author Contributions: Conceptualization A.E. and L.K.; Formal analysis L.K.; Funding acquisition A.E.; Investigation L.K.; Methodology A.E. and L.K.; Supervision A.E.; Writing—original draft A.E. and L.K.; Writing—review & editing A.E. and L.K. All authors read and agreed to the published version of the manuscript.

Funding: This research was supported by the Ontario Research Fund—Research Excellence (ORF-RE Round 8).

Institutional Review Board Statement: Not Applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The data presented in this study are openly available in Mendeley Data at 10.17632/fngtzjdy95.1, reference number [17].

Acknowledgments: The authors would like to thank Katarina Grolinger, Shaimaa Ali, Anwar Sedig, and the anonymous reviewers for their valuable feedback.

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript:

BLE	Bluetooth Low Energy
CVSS	Common Vulnerability Scoring System
GAEN	Google Apple Exposure Notification
OS	Operating System
SIG	Special Interest Group

Appendix A. App Attack Analysis Example, Canada Covid Alert

We performed the vulnerability analysis for the 18 attacks against each of the 5 representative applications. Below is an example of the reasoning for the score given. This is the analysis of the first attack against the Canadian Covid Alert application. Due to length limitations, the entire scoring procedure for all of the apps could not be included in this paper. The analysis of each attack against each app can be found in [17].

Attack 1

- **Access: 2/10**. There is nothing in the protocol to prevent someone from building a tool to collect GPS location data when the phone makes a BLE connection. The attack requires either circumventing the app to log the contact information outside of it or rooting the attackers device to access the logged contact information. The bottleneck of attack 1 is obtaining the temporary IDs of the victim to trace through the system. In the Covid Alert documentation, all it says is that the temporary IDs are "securely stored" without a clear definition of what that means [22]. It is assumed that to see the temporary IDs, the attacker would need to root the victims device. Thus, this attack should be marked as a 1. However, because the IDs of positive users are made available through the server, an attacker could collect all of this information, and then recreate the list of IDs of positive users, find matches and follow them. This possibility is why the score is a 2.

- **Knowledge: 3/10**. The attack would require being able to make the GPS logging code, detect that the device has logged the Bluetooth information, root the attacker's own device and potentially the victims, or pull the list from the server and recreate the IDs of positive users.
- **Complexity: 6/10**.
  - **Technology: 7/10**. The tools required for the exploit would require a standard computer to create. The analysis can be done on a consumer computer.
  - **Build: 5.** The attack requires one or two tools, the GPS logger, the access to the contact list, and the method of collecting the IDs to track. Then, the program matches the ID and every GPS coordinate and maps them together. One person could do this in more than a month, or a few could do this in about a month. All of these components were created before for GPS-based data attacks and would need to be put together for this.
- **Effort: 1.5/10**.
  - **Planning: 1/10**. This is high effort because the code has to be placed on many phones to collect all of the required information. Then, the data have to be compiled.
  - **Human: 2.** To effectively cover an area, quite a few people would need to be involved. Once the software is on their phone, they would not have to necessarily do anything out of the ordinary however, just go through their usual routine.
- **Scope: 4/10**. This would affect the group that the IDs could be identified for. People close to any of those involved whose devices could be accessed to obtain the IDs or people who test positive in the community. This is smaller than everyone that an attacker knows and is not every positive individual, as it is relegated to the area covered.
- **Impact: 4/10**.
  - **Data: 4/10**. The contact log information itself is not easy to use, but the GPS data allow the creation of a map of where someone has been and could then determine where they live, work, or other personal information.
  - **Trust: 4/10**. This would damage trust in the system. There is the potential that a politically motivated group could use this to single out certain people, especially if they can target those that have the virus.
- **Detection: 8/10**. It is possible that this would not be noticed. The code that collects the information does not need to interfere with the app, just monitor it; however, the amount of people involved would require quite the vow of secrecy. It could involve access to someone's phone to retrieve the IDs, which would increase the risk of detection.
- **Repairability: 2.5/10**.
  - **System: 1/10**. The code added to the groups devices would have to be removed, but otherwise, the system itself has not truly been touched.
  - **User: 4/10**. The damage solely from this vulnerability would not be permanent, but harmful to someone's privacy, as they would have been tracked.

Average: 3.875

References

1. Lomas, N. Norway Pulls Its Coronavirus Contacts-Tracing App after Privacy Watchdog's Warning. *TechCrunch* **2020**. Available online: https://techcrunch.com/2020/06/15/norway-pulls-its-coronavirus-contacts-tracing-app-after-privacy-watchdogs-warning/ (accessed on 10 June 2021).
2. Government of Singapore. Blue Trace Protocol. *bluetrace.io* **2020**. Available online: https://bluetrace.io/ (accessed on 10 May 2021).
3. Apple Inc. Exposure Notification Framework. *Apple Dev. Doc.* **2020**. Available online: https://developer.apple.com/documentation/exposurenotification (accessed on 10 May 2021).
4. Luccio, M. Using contact tracing and GPS to fight spread of COVID-19. *GPS World*, 3 June 2020.

5. UK NHS. What the App Does. *NHS COVID-19 App Support* **2020**. Available online: https://covid19.nhs.uk/what-the-app-does.html (accessed on 10 June 2021).
6. Mozur, P.; Zhong, R.; Krolik, A. In Coronavirus Fight, China Gives Citizens a Color Code, With Red Flags. *The New York Times*, 1 March 2020.
7. Johns Hopkins Coronavirus Resource Center. COVID-19 Map. 2020. Available online: https://coronavirus.jhu.edu/map.html (accessed on 10 March 2021).
8. Sweeney, L. *Simple Demographics Often Identify People Uniquely*; Carnegie Mellon University: Pittsburgh, PA, USA, 2000.
9. Tockar, A. *Riding with the Stars: Passenger Privacy in the NYC Taxicab Dataset*; Neustar Research: Sterling, VA, USA, 2014.
10. Drakonakis, K.; Ilia, P.; Ioannidis, S.; Polakis, J. Please Forget Where I Was Last Summer: The Privacy Risks of Public Location (Meta)Data. *CoRR* **2019**, abs/1901.00897.
11. Díaz, C.; Seys, S.; Claessens, J.; Preneel, B. Towards Measuring Anonymity. In *Privacy Enhancing Technologies*; Dingledine, R., Syverson, P., Eds.; Springer: Berlin/Heidelberg, Germany, 2003; pp. 54–68.
12. Serjantov, A.; Danezis, G. Towards an Information Theoretic Metric for Anonymity. In *Privacy Enhancing Technologies*; Dingledine, R., Syverson, P., Eds.; Springer: Berlin/Heidelberg, Germany, 2003; pp. 41–53.
13. Alderson, E. Aarogya Setu: The Story of a Failure. *Medium* **2020**. Available online: https://medium.com/@fs0c131y/aarogya-setu-the-story-of-a-failure-3a190a18e34 (accessed on 10 June 2021).
14. Amnesty International. Major Security Flaw Uncovered in Qatar's Contact Tracing App. *Amnesty Int.* 2020. Available online: https://diaspora.evforums.net/posts/ecc5380081860138a774005056264835 (accessed on 26 May 2020).
15. Hamilton, I.A. Cybersecurity Experts Found Seven Flaws in the UK's Contact-Tracing App. *Bus. Insid.* 2020. Available online: https://www.businessinsider.com/cybersecurity-experts-find-security-flaws-in-nhs-contact-tracing-app-2020-5 (accessed on 20 May 2020).
16. Goodes, G. REPORT: Most Government-Sanctioned Covid-19 Tracing Apps Risk Exposing Users' Data and Privacy. 2020. Available online: https://www.guardsquare.com/blog/report-proliferation-covid-19-contact-tracing-apps-exposes-significant- security-risks (accessed on 16 June 2020).
17. Krehling, L.; Essex, A. Support Document for "A Security and Privacy Scoring System for Contact Tracing Applications". *Mendeley Data* **2021**, *1*. [CrossRef]
18. Wikipedia. COVID-19 Apps. Available online: https://www.wikipedia.org/ (accessed on 13 March 2021).
19. Rahman, M. Here Are the Countries Using Google and Apple's COVID-19 Contact Tracing API. 2020. Available online: https://www.xda-developers.com/google-apple-covid-19-contact-tracing-exposure-notifications-api-app-list-countries/ (accessed on 13 March 2021).
20. FIRST. CVSS v3.1 Specification Document. *FIRST* **2015**. Available online: https://www.first.org/cvss/v3.1/specification-document (accessed on 10 April 2021).
21. Kerschbaum, F.; Barker, K. Coronavirus Statement. *Waterloo Cybersecur. Priv. Inst.* **2020**. Available online: https://uwaterloo.ca/cybersecurity-privacy-institute/news/coronavirus-statement (accessed on 10 April 2021).
22. Office of the Privacy Commissioner of Canada. *A Framework for the Government of Canada to Assess Privacy-Impactful Initiatives in Response to COVID-19*; Office of the Privacy Commissioner of Canada: Ottawa, QC, Canada, 2020.
23. Gillmor, D.K. *ACLU White Paper—Principles for Technology-Assisted Contact-Tracing*; American Civil Liberties Union: New York, NY, USA, 2020.
24. Club, C.C. 10 Requirements for the Evaluation of "Contact Tracing" Apps. 2020. Available online: https://www.ccc.de/en/updates/2020/contact-tracing-requirements (accessed on 10 April 2021).
25. Ministry of Electronics & Information Technology. AarogyaSetu Bug Bounty Programme (for Android App). *Bug Bounty Program* **2020**. Available online: https://static.mygov.in/rest/s3fs-public/mygov_159057669351307401.pdf (accessed on 10 June 2021).
26. Health Canada. Canada's Exposure Notification App. 2020. Available online: https://www.canada.ca/en/public-health/services/diseases/coronavirus-disease-covid-19/covid-alert.html (accessed on 10 June 2021).
27. The Directorate of Health and The Department of Civil Protection and Emergency Management. The Directorate of Health and The Department of Civil Protection and Emergency Management (Iceland). Privacy policy Rakning C-19—App. *Upplýsingar um Covid-19 á Íslandi*. 2020. Available online: https://www.covid.is/app/protection-of-personal-data (accessed on 1 June 2021).
28. National Informatics Center of India. *Aarogya Setu* **2020**. Available online: https://aarogyasetu.gov.in/technical-faqs/ (accessed on 10 June 2021).
29. PRIVATICS Team—Inria and Fraunhofer AISEC. ROBust and privacy-presERving proximity Tracing protocol. 2020. Available online: https://github.com/ROBERT-proximity-tracing/documents (accessed on 1 May 2021).
30. Aranja. Rakning-c19-App. *GitHub* **2020**. Available online: https://github.com/aranja/rakning-c19-app (accessed on 10 June 2021).
31. The Government of Canada. COVID Alert Privacy Notice (Google-Apple Exposure Notification). *Canada.ca*, 9 February 2021. Available online: https://www.canada.ca/en/public-health/services/diseases/coronavirus-disease-covid-19/covid-alert/ privacy-policy.html (accessed on 1 May 2021).
32. Office of the Privacy Commissioner of Canada. *Privacy Review of the COVID Alert Exposure Notification Application*; Office of the Privacy Commissioner of Canada: Ottawa, QC, Canada, 2020.
33. Government of France. TousAntiCovid Application. *Gouvernement.fr*, 11 May 2021. Available online: https://www.gouvernement.fr/info-coronavirus/tousanticovid (accessed on 1 May 2021).

34. Government of France. Help for Using TousAntiCovid. *Tousanticovid.stonly*. 5 March 2021. Available online: https://tousanticovid.stonly.com/kb/fr/donnees-personnelles-26615 (accessed on 1 May 2021).
35. National Informatics Center of India. Aarogya Setu FAQ's. *Aarogya Setu* **2020**. Available online: https://aarogyasetu.gov.in/faq/ (accessed on 10 June 2021).
36. Clarance, A. Aarogya Setu: Why India's Covid-19 Contact Tracing App Is Controversial. *BBC News*, 15 May 2020.
37. Government of India. *Aarogya Setu* **2020**. Available online: https://www.aarogyasetu.gov.in/ (accessed on 10 June 2021).
38. Government of Singapore. *OpenTrace* **2020**. Available online: https://github.com/OpenTrace-community (accessed on 10 June 2021).
39. Asher, S. TraceTogether: Singapore turns to wearable contact-tracing Covid tech. *BBC News*, 5 July 2020.
40. Government of Singapore. TraceTogether Privacy Safeguards. *TraceTogether*, 1 April 2020.
41. Google; Apple Inc. Exposure Notifications: Using Technology to Help Public Health Authorities Fight COVID-19. *Covid-19 Information & Resources*. Available online: https://www.google.com/search?q=privacyinformationgain&rlz=1C1CHBF_enCA960CA961&oq=privacyinformationgain&aqs=chrome..69i57j33i160.3632j1j7&sourceid=chrome&ie=UTF-8 (accessed on 10 June 2021).
42. Sun, R.; Wang, W.; Xue, M.; Tyson, G.; Camtepe, S.; Ranasinghe, D. Vetting Security and Privacy of Global COVID-19 Contact Tracing Applications. *CoRR* **2021**, arXiv:2006.10933v3.
43. Sowmiya, B.; Abhijith, V.; Sudersan, S.; Sundar, R.S.J.; Thangavel, M.; Varalakshmi, P. A Survey on Security and Privacy Issues in Contact Tracing Application of Covid-19. *SN Comput. Sci.* **2021**, *2*, 136. [CrossRef] [PubMed]