Supporting Contact Tracing by Privacy-Friendly Registration at Catering Facilities

Michiel Willocx
imec-DistriNet
Gebroeders Desmetstraat 1
9000 Gent, Belgium
michiel.willocx@kuleuven.be

Dave Singelée
imec-COSIC
Kasteelpark Arenberg 10
3001 Heverlee, Belgium
dave.singelee@esat.kuleuven.be

Jorn Lapon
imec-DistriNet
Gebroeders Desmetstraat 1
9000 Gent, Belgium
jorn.lapon@kuleuven.be

Vincent Naessens
imec-DistriNet
Gebroeders Desmetstraat 1
9000 Gent, Belgium
vincent.naessens@kuleuven.be

ABSTRACT
The corona virus has hit the world with an unprecedented global pandemic, forcing many countries around the world in a lockdown with social distancing measures. Along with a wide range of hygienical measures such as wearing masks and washing hands, contact tracing solutions aim at reacting quickly to new infections. Two approaches are widely employed in an attempt to control the spreading of the corona virus, namely permanent contact tracing and hospitality unit registration. For permanent contact tracing, privacy-friendly solutions such as DP-3T are available. However, for the mandatory hospitality unit registration, current (digital) solutions remain rather primitive and do not offer satisfying privacy properties. This work proposes a privacy-preserving, digital solution for the mandatory registration in bars and restaurants while satisfying the needs of governmental institutes, the customer and the bar owners.

CCS Concepts
•Security and privacy ~ Cryptography • Security and privacy ~ Security services ~ Privacy-preserving protocols • Security and privacy ~ Security services ~ Pseudonymity, anonymity and untraceability

Keywords
Security, privacy, covid-19, contact tracing.

1. INTRODUCTION
At the start of 2020, the world was hit by an unprecedented global pandemic. The pandemic, caused by the corona virus, was able to spread around the world in no time. Countries were forced into a lockdown with major social distancing regulations in order to avoid an overdemand of medical care in hospitals. After the first wave, lockdown and social distancing measures were relaxed again. However, as long as no vaccine is available, new infections waves are a serious threat. To mitigate the threat, it is of major importance that new infection sources are detected as soon as possible, and that potentially infected citizens are warned in order to decrease the spread.

Governments all over the world are taking measures to limit the exposure of the virus to society. Technological support for contact tracing can play a key role to control the serious threats. Contact tracing systems are being deployed, allowing citizens to receive warnings when a potential infection has taken place. While there is no doubt that these systems have a positive impact on the situation, many infection sources remain untraceable. Therefore, additional measures have been taken. Many governments impose hospitality facilities to register all customers. In the beginning, digital support was lacking, forcing the majority of bars and pubs to perform this registration with pen and paper. After a few weeks, digital tools were made available by local governments and SMEs. While these digital solutions can drastically increase the accuracy and ease-of-use, many of them hardly tackle imperative security and privacy concerns.

Contribution. This work proposes a privacy-preserving digital solution for the mandatory registration in bars and restaurants. Our approach aligns the concerns of the major stakeholders in this setting. Firstly, governments that put this mandatory registration in place want correct information that enables them to contact and warn uninformed but possibly infected citizens. Secondly, the restaurant owners want to be able to have business as usual with minimal overhead. Lastly, privacy is a major concern from the perspective of citizens. At the same time, they wish to receive useful and reliable information from the system (e.g. information about infection sources that may be relevant for them).

The remainder of this paper is structured as follows. Section 2 sketches the landscape of existing contact tracing solutions. Next, Section 3 enumerates the requirements of our registration solution. This is followed by an outline of the security assumptions are were taken during the design stage of our solution in Section 4. The design itself is presented in Section 5 and evaluated in Section 6. This is followed by a discussion of alternative solutions in Section 7, and conclusions in Section 8.

2. RELATED WORK
Two approaches are currently employed in an attempt to control the spreading of the corona virus, namely *permanent contact tracing* and *hospitality unit registration*. Permanent tracing systems [1, 2, 3] continuously monitor encounters between citizens, either location-based or proximity-based. People that came into possible physical contact with a covid infected person are warned. Furthermore, contact tracing data can also be applied by researchers and governments to assess high risk areas and infection patterns.

Hospitality tracing systems register individuals visiting pubs, bars, restaurants or hotels, and warn people about a possible exposure to a covid infected person. Hospitality tracing is enrolled in many countries and regions and is often mandatory [4, 5, 6].

2.1 Hospitality Tracing Systems

Currently, many pubs and restaurants still rely on pen and paper to perform hospitality registration. However, many challenges arise when doing so. The pens are handled by many customers and bar personnel, implying that the whole procedure is unhygienic and, hence, unsafe. Moreover, the approach is error prone and unreliable, as handwritings are often unreadable, and it is hard to verify the authenticity the provided information. Straightforward digital software solutions are developed by governments and SMEs [7, 8] that enable public restaurants and pubs to meet the mandatory registration of guests. These systems often consist of a simple web form that replaces pen and paper. In most cases, this form is just sent to a central database hosted by the developer of the form. Although digital solutions are more hygienic, verifying the authenticity of the information remains hard. Moreover, those systems expose serious privacy threats by design, as all information is collected and stored in one central database, often managed by one commercial organization. This centralized design principle also increases the risk of potential data leakage breaches.

2.2 Location Tracing Systems

Location based systems rely on absolute GPS locations to match locations of users. They apply surveillance strategies in order to enable digital contact tracing. Such systems are enrolled in China and South Korea [9, 10]. This strategy is undoubtedly highly privacy invasive as the government has location data of each citizen at all times. Those data are sometimes enriched with data from public cameras and biometric data. Besides warning possibly infected people, these systems are also used to track and control known infected patients. For example, China employs a QR code system in public places and public transport that denies citizens that are classified by the system as high risk patients [11, 12].

2.3 Proximity Tracing Systems

In contrast to location tracing systems, proximity based systems use communication technologies such as Bluetooth in order to assess interactions between potentially infected citizens. Privacy was a major concern in many designs of proximity tracing systems. Instead of building huge centralized databases filled with private information on citizens, decentralized systems are built that store information only locally on the users' device and apply cryptographic techniques that mask the identity of its users. Multiple alternatives [13, 14, 15] have been proposed and are currently deployed. The main idea is that each user's device generates (unidentifiable) tokens that are broadcast in fixed time intervals. Other devices within Bluetooth range pick up and store these tokens. When a citizen is diagnosed with covid, he releases his tokens to a governmental database (without leaking his identity). To assess potential exposure, all users periodically download the list of tokens of infected people and compare them to the tokens stored on their device. Some systems rely on operating system support to enable the application's functionality. Both Apple and Android have released an SDK [16, 17] to support this category of contact tracing apps. Applications require a special permission from Apple and Google to access this SDK, and the SDK will be automatically disabled after the pandemic.

While proximity-based contact tracing apps are valuable yet privacy-friendly tools for risk-assessment, some challenges remain. Firstly, even countries with a contact tracing application still have trouble finding the source of an infection in many cases [18, 19]. The reason behind this is that privacy friendly contact tracing apps only reveal a list of identifiers corresponding to infected persons (assuming that the infected persons comply and actually report all their identifiers). One solely relies on the app of the user to link the identifiers to specific locations, and there is no way for external parties to verify this. Next, contact tracing apps cannot replace the mandatory registration systems in pubs and restaurants. The decentralized contact tracing system is not designed to force individuals to actually register at a specific location (or even to enforce that a temporary identifier is actually transmitted or received). Many proximity tracing systems cannot verify if users that were in proximity of possibly infected individual, are actually informed. Lastly, permanent Bluetooth connection has a negative impact on the battery usage of the device which can decrease the amount of people willing to install the app.

Therefore, it is not possible to reuse existing contact tracing solutions for mandatory registration at catering facilities. There is a clear need for a novel, privacy-preserving solution to tackle this challenge. This paper presents a privacy-friendly solution for mandatory registration in pubs and restaurants. The work presented in this paper can be used complementary to proximity tracing applications.

3. REQUIREMENTS

3.1 Governmental Directives

The application must be compliant with governmental directives related to contact tracing. In many countries and regions, governments stipulate mandatory registration when individuals enter a catering facility. Our system aims at providing a privacy friendly yet easy-to-deploy alternative to roll out this mandatory catering facility registration, and is complementary to proximity tracing apps that are often on a voluntary basis.

3.2 Effectiveness and Efficiency

(E1) The registration procedure must be straightforward both from the perspective of the proprietor and the consumer. (E2) Users must be informed if they were present at the same location and time as a covid infected person. This must happen efficiently. This means that the manual intervention of contact tracers must be limited to a bare minimum (i.e., users only receive a phone call when they did not confirm an electronic notification for some time). (E3) The government must get an overview of facilities that were visited by covid infected individuals. This is of major importance to keep the virus under control.

3.3 Privacy

(P1) No entity can link the identity of visitors to locations except when exposed by the person itself (e.g. posted on social media). (P2) Only the location of infection sources can be revealed, and only to a trusted entity (e.g. a dedicated governmental institution) and the visitors of that location during the vulnerable time interval. (P3) The identity of visitors is never revealed, even if they are possibly infected, unless they remain uninformed during a predefined time interval. If so, the system must be able to deanonymize the visitor to contact her. (P4) Noone can learn how long a user has spent in a catering facility.

3.4 Security

(S1) Users may not be able to falsely claim that they are infected. The matching service will only process claims that are approved by a general practitioner. (S2) Users may not be able to falsely claim to have visited a catering facility that they didn't visit. (S3) Users

only retrieve a notification about the source of infection if they were present at that location during a vulnerable time interval. (S4) The system knows at any time whether exposed users are informed or not. (S5) The system must be able to cope with Denial-of-Service attacks. Users may not be able to flood the database of the matching service with fake location data. (S6) A user cannot falsely claim to have performed the mandatory registration at the catering facility. (S7) Catering facilities that have tampered with the registration system, can be detected.

3.5 Technological Demands

(T1) The catering facilities do not need to enroll a complex digital infrastructure or perform complex interactions to verify the mandatory user registration during check-in. (T2) Users must only download a mobile app and go through a simple registration procedure. (T3) The solutions impose minimal constraints on battery power, processing power and communication overhead. (T4) The solution does not rely on Bluetooth and does not require collaboration of mobile platform providers such as Apple and Google.

4. SECURITY ASSUMPTIONS

The following security assumptions were made during the design of our solution. (A1) None of the parties in the system collude. (A2) All the services (i.e., registrars, mix and matching service) in the system are assumed to be honest but curious. (A3) The user can tamper with its mobile phone. (A4) The catering facility can tamper with its registration system. (A5) An anonymous communication channel can be setup between the user and the mixing server, that does not leak any information on the user's identity. Moreover, the users know the public key of the mixing server (e.g., pre-installed in the app). (A6) The communication between all the services in the system is secured. All these services know each other's public key.

5. PROPOSED SOLUTION

Figure 1 gives an overview of the different roles and their interactions. Six roles can be distinguished in the system. A catering facility can be a pub, a restaurant or a hotel. The catering facility relies on a QR code to support user registration. A user is each person that can visit catering facilities. A user needs to register when entering a catering facility and must be informed if an infected person was at the catering facility at the same time interval. The general practitioner examines people with symptoms and initiates the contact tracing procedure when a patient is diagnosed as 'covid infected'. The other roles are explicitly defined to support contact tracing. The registrar has three major tasks. First, it enrolls new catering facilities and provides them with a tool to generate QR codes on a daily basis. Second, it enrolls new users and provides them with tokens that can be used when visiting a catering facility. Third, it reveals contact information of possibly infected people. The matching service keeps information about visits and supports contact tracing. Note that uniquely identifying user and catering facility data are not revealed to the matching service.

Besides those key roles, a mix proxy shuffles incoming messages (i.e. capsules - see further) and flushes them at regular time intervals to the matching service. Further, a central health authority (not included in figure 1) mediates interactions between the general practitioner and the matching service.

Five phases can be distinguished. During enrollment, users and catering units register to the system. The second phase includes the steps that are taken when a user visits a catering facility. Phase three focuses on the flow that is initiated when a patient is diagnosed as covid infected by a general practitioner. Next, we show how visitors are informed about their risk status (phase four). Finally, random spotchecks are discussed.

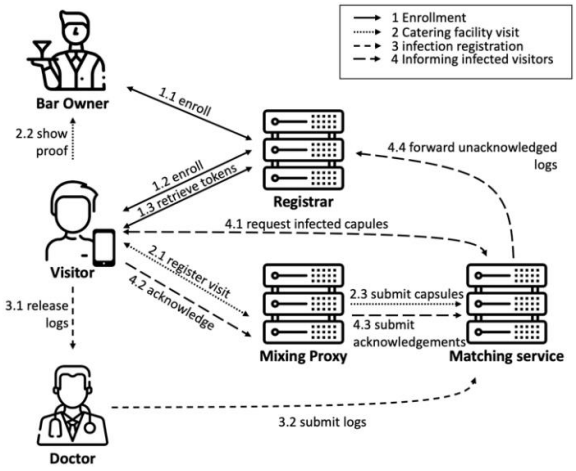

Figure 1. Interaction flow between stakeholders.

5.1 Enrollment

Both catering facilities and users need to enroll in the system.

Catering Facility Enrollment. The former interacts with a web service provided by the registrar. The latter generates a master secret key s. Each catering facility exposes uniquely identifying information (e.g., unique business number, name and address of the facility, and/or phone number) and the authenticity thereof. The registrar then derives each day_i a new secret key s_{CF,day_i}, based on a unique identifier CF of the catering facility that is calculated as follows (with KDF being a secure key derivation function):

$$s_{CF,day_i} = KDF(s, CF, day_i).$$

Next, it calculates a day-specific pseudonym nym_{CF,day_i} for the catering facility as follows (with H being a cryptographic hash function):

$$nym_{CF,day_i} = H(s_{CF,day_i}, location_{CF}, day_i)$$

The pseudonym nym_{CF,day_i} is sent to the catering facility ultimately at the start of that particular day. Note that for efficiency reasons, a set of pseudonyms can be sent in batch (e.g., at the beginning of each month). The application running at the catering facility CF then generates a random number R_i and a new QR code on a daily basis that contains three values:

$$QR_{CF,day_i} = [R_i, CF, H(R_i, nym_{CF,day_i})]$$

User Enrollment. An individual first downloads a covid-catering app from a trustworthy app store. After installation, the user needs to go through an enrollment phase which is bound to the phone number. That number can act as unique identifier and prevents users from enrolling many times. After successful enrollment, the registrar issues a set of signed tokens to each user. Each token $T^{user}_{x,day_i} = sign_{RC}(random, day_i)$ can be spent exactly once, at a catering facility. Although other time windows can be used, our prototype issues 48 tokens a day to each user. Note that the registrar keeps the mapping between the phone number and the tokens that

were issued. None of the other parties in the system is able to derive the identify of the user from a token.

5.2 Visiting a Catering Facility

We assume that each pub, hotel or restaurant shows her QR code QR_{CF,day_i} at a clearly visible location (e.g., at the entrance of the facility or attached to each table). The code is valid during one day. When a visitor enters the facility, she scans QR_{CF,day_i} and logs the three values R_i, CF and $H(R_i, nym_{CF,day_i})$ exposed by the QR code together with the entry time locally on the phone, for a specific number of days. The duration depends on the governmental directives and is related to the incubation time of the virus. The app then registers the visit by sending a *capsule* to the mixing server via a secure connection with server authentication activated. This capsule contains the current time interval, a valid user token T^{user}_{x,day_i} and the 3rd value in the QR code (i.e., $H(R_i, nym_{CF,day_i})$). Note that R_i and CF remain locally on the phone of the visitor. Upon receiving a capsule, the mixing server first checks (a) the validity of the user token, and then verifies that (b) it is a token for that particular day_i and (c) it has not been spent before. If all three checks are successful, the mixing server signs $H(R_i, nym_{CF,day_i})$ and sends it back as confirmation to the app of the user. The app then transforms the bits of the signature to a visual representation. This can be a symbol with a specific color -- or a variant -- and the current time interval. As all customers receive the same signature, the facility manager can easily verify this visual representation of this signed acknowledgement (as the facility manager has also received the symbol when he registered that day as the first customer). As such, the facility manager is convinced that the app has really sent the third value and a user token to the mixing server.

The user can show the visual representation to the catering personnel when doing a first order (and optionally at subsequent orders). Depending on local directives either one individual per bubble or all individuals scan the code.

Every time the app sends a capsule to the mixing server (i.e. two times an hour in our prototype), the mixing server adds the time to this entry. This way, users cannot lie about the time he has visited that location. The user is prevented from delaying the transmission of an entry to the mixing server, as the catering facility demands a proof (i.e. the visual code) that the capsule was sent correctly to the mixing server.

The mixing server holds the capsules of all users during some time interval. Shortly after the time interval has finished, the capsules are flushed to the matching service in a random order. The data is removed from the database of the matching service after a predefined time interval, which can be imposed by the government (with a minimum of one day to prevent multiple spending of the same user token).

When a user leaves the catering facility, the smartphone logs the exit time. The user can push a button in the app when exiting, or the waitress forces the users to take an action. Alternatively, an app notification can be sent to the user when he leaves the facility. Geo-fencing can be used to detect users leaving a certain location.

5.3 Registering an Infected User

When feeling sick, a user should visit a practitioner who can diagnose that a user is covid infected. If so, the practitioner reads out part of the users' logs (i.e. T^{user}_{x,day_i}, $H(R_i, nym_{CF,day_i})$ and R_i) and the time intervals that were stored on the smartphone. He signs and forwards these via the central health authority to the matching service, possibly after shuffling them with tuples of other users. The matching service downloads all nym_{CF,day_i} for a particular day from the registrar. Once the matching service knows all day-specific pseudonyms nym_{CF,day_i}, it has all information required to control the validity of the data provided by the user by taking hashes of R_i *and* the registrar's identifier CF. Hence, the latter cannot lie about his locations, as he cannot provide a valid R_i for places he did not visit. As long as a user does not report about his locations, someone that did not scan the QR code cannot retrieve the location (as the location cannot be revealed without knowledge of R_i).

The matching server marks all entries that contain capsule data for that facility $[H(R_i, nym_{CF,day_i}), interval]$ as 'critical', and marks the token T^{user}_{x,day_i} of the infected user (that visited the general practitioner) as 'informed'. All other tokens in the same entry are 'uninformed'.

5.4 Informing Possibly Infected Users

Once a day, each user (i.e. the smartphone app) fetches a list of fresh critical tuples $[H(R_i, nym_{CF,day_i}), interval]$. The app checks whether the tuples also appear in its local storage. This would mean that the user was at a particular location within the critical time interval. If so, the user picks the corresponding $token(s)$ T^{user}_{x,day_i} and sends these to the mixing proxy which further forwards it to the matching service. The matching service marks all confirmed tokens as 'informed'. After a certain time interval (e.g., one day), the remaining tokens are forwarded to the *registrar*. The latter contacts all 'uninformed' people that were at the facility at the critical time interval.

5.5 Random Spotchecks

To prevent that a catering facility cheats and does not show the right QR code to its customers, the catering facility registrar performs random spotchecks. Therefore, an agent of the registrar visits a catering facility and scans the QR code. As the registrar knows the pseudonym of each catering facility beforehand, it can immediately check the validity of the QR code when scanning it.

6. EVALUATION

This section reflects about the security and privacy properties of the presented hospitality facility registration system.

6.1 Privacy

One of the main privacy requirements of the proposed system is that none of the services in the system can reveal the identity of the other users in the system, besides the registrar. This requirement is satisfied, as only the registrar can link the user tokens to the actual users. The registrar will only reveal the identity of the users to the matching server for the tokens that have not been claimed by the user in case of an infection. It should be noted that the system does not provide unlinkability. Both the mixing server and the matching server can detect that specific entries are linked to the same location. However, besides not being able to learn the identities of the users that visited that location, none of these parties can learn the exact location. This property is achieved due to the one-way property of the hash function and the random number R_i that is only revealed when an infected person reports to the health authorities. The entries that are sent to the mixing server do not reveal any information about the pseudonym of the catering facility. The distinct entries cannot be distinguished from random bit strings. Note that the mechanism deployed in our solution is similar to a commitment. As long as R_i is not revealed, the information is

hidden. Once R_i is revealed, one cannot change the content of the capsule (e.g., link it to another catering facility). When an infection is detected, the user reveals the location entries stored in the app, and hence reveals the values R_i and the catering facility pseudonym. The catering facility registrar can then, using this pseudonym, inform the matching server about the identity and location of the corresponding catering facility.

6.2 Security

The security requirements presented in Section 3 are defined to prevent that malicious stakeholders can cheat the system.

Catering facilities can display fake QR codes to hide the name of the location under any circumstances. However, random spot checks with possible fines should discourage malicious behaviour. If the spot check inspector reads the QR code, the random value $R_i$is disclosed. Hence, the inspector can verify the validity of the QR code (using the nym_{CF,day_i} of that catering facility).

Users could attempt to bypass the system, insert false information in the system, or attempt to flood it with meaningless input. When entering a catering facility, a customer must scan the QR code of the catering facility. The user is forced to register his visit. Thereby, she must rely on data included in the QR code. These data are required in order to receive a correct signature from the mixing server. Before a first order, the bartender can check the signature. The user cannot know this value (i.e. the signature on the entry of the QR code) in advance, and hence can hardly bypass the registration. Bypassing would mean that the visitor mimics the interface of the app, eavesdrops the visual representation of the signature from another visitor of that same catering facility and displays it in the counterfeited app. Flooding is prevented by restricting the amount of tokens a user can acquire each day. Each token can only be spent once, preventing malicious users to flood the database. Inserting false information is prevented by the random R_i included in the QR code. When an infected user releases his logs to the practitioner, he cannot lie about the facilities he visited. For each capsule that is released, the user has to provide the values R_i and the pseudonym that were included in the QR code. And a user cannot know the pseudonyms of other locations, nor find another value R_i' and false pseudonym such that the hash function corresponds to the value that was sent before in the capsule. For all capsules that are not used, the impact of a false capsule is minimal (as it is just deleted after a certain time interval and never used). Lastly, false infections cannot be introduced in the system. Only capsules that are signed by the general practitioner will be accepted by the health authorities and the matching server.

7. DISCUSSION

The proposed solution satisfies all predefined requirements. This section discusses alternative designs and possible extensions to the proposed solution.

It should be noted that many requirements in our approach can also be met by extending proximity tracing solutions such as DP-3T [13] with location information. However, other requirements are hard to achieve by just extending DP-3T. Firstly, users must be contacted by externals (e.g. a health authority call center) after some time if they remain uninformed yet critical. Secondly, registration is mandatory and must be reliable. It involves collaboration of visitors as well as catering facilities. Thirdly, in contrast to proximity tracing, our approach releases useful data to researchers and governmental instances to study the spread of the virus without impacting the privacy of end-users.

Using more complex cryptographic building blocks, privacy could further be enhanced. For instance, to prevent a colluding registrar and matching service to obtain the identity of the users in the database, an oblivious third party, as discussed by Camenisch et al. [20], could be used. In short, the signed tokens would be (verifiably) encrypted such that an oblivious third party only decrypts the signed token if the user did not publish a confirmation for that token (on a public bulletin board). Note that this would make other steps in the protocol more involved, as to ensure that one can verify that the encrypted tokens were issued by the registrar and to prevent double spending or a Denial-Of-Service attacks.

Finally, the proposed system can also be deployed in other settings. One example is controlling the spread of diseases during animal transport at an early stage. Information like the identifier and owner of the animal, mode of transportation and current residency can be hidden towards the matching service similarly to the way user information and the hospitality location are hidden in our approach.

8. CONCLUSIONS

This paper presented a privacy-friendly alternative for the mandatory registration for pub and restaurant guests. The solution satisfies both the governmental requirements and the privacy requirements of the visitors while reducing the overhead for hospitality management to an absolute minimum. The identity of the hospitality units and the visitors are never disclosed unless an infection occurs. Even in this case, the identity of the potentially infected visitor is only revealed when the automatic infection message is not acknowledged by that user after a certain time frame.

9. REFERENCES

[1] Ferretti, Luca, et al. , "Quantifying SARS-CoV-2 transmission suggests epidemic control with digital contact tracing.," *"Contact tracing and disease control." Proceedings of the Royal Society of London. Series B: Biological Sciences.*

[2] Eames, Ken TD, and Matt J. Keeling., "Contact tracing and disease control.," *Proceedings of the Royal Society of London. Series B: Biological Sciences 270.1533 (2003): 2565-2571.*.

[3] Klinkenberg, Don, Christophe Fraser, and Hans Heesterbeek, "The effectiveness of contact tracing in emerging epidemics.," *PloS one 1.1 (2006): e12.*

[4] "Belgium Corona measures," [Online]. Available: https://www.vrt.be/vrtnws/en/2020/07/23/national-security-council/. [Accessed 4 August 2020].

[5] "Berlin Corona measures," [Online]. Available: https://www.berlin.de/corona/en/measures/. [Accessed 4 August 2020].

[6] "UK Corona measures," [Online]. Available: https://www.gov.uk/guidance/maintaining-records-of-staff-customers-and-visitors-to-support-nhs-test-and-trace. [Accessed 4 August 2020].

[7] "telegraph - mandatory registration," [Online]. Available: https://www.telegraph.co.uk/news/2020/06/21/pubs-restaurants-register-customers-contact-details-track-trace/. [Accessed 4 August 2020].

[8] "NSW Corona Measures," [Online]. Available: https://www.nsw.gov.au/media-releases/tough-new-covid-19-compliance-measures-for-pubs. [Accessed 4 August 2020].

[9] Klimburg, Alexander, Louk Faesen, and P. Verhage., "Pandemic mitigation in the digital age: digital epidemiological measures to combat the coronavirus pandemic.," *The Hague Centre for Strategic Studies.*

[10] "A flood of coronavirus apps are tracking us. Now it's time to keep track of them.," MIT Technology Review, [Online]. Available: https://www.technologyreview.com/2020/05/07/1000961/launching-mittr-covid-tracing-tracker/. [Accessed 5 August 2020].

[11] "China's coronavirus health code apps raise concerns over privacy," The Guardian, [Online]. Available: https://www.theguardian.com/world/2020/apr/01/chinas-coronavirus-health-code-apps-raise-concerns-over-privacy. [Accessed 5 August 2020].

[12] "South Korea is watching quarantined citizens with a smartphone app," MIT Technology Review, [Online]. Available: https://www.technologyreview.com/2020/03/06/905459/coronavirus-south-korea-smartphone-app-quarantine/. [Accessed 5 August 2020].

[13] "DP-3T -- Decentralized privacy-preserving proximity tracing," [Online]. Available: https://github.com/DP-3T/documents. [Accessed 4 August 2020].

[14] "Covid Watch," [Online]. Available: https://www.covid-watch.org/article. [Accessed 4 August 2020].

[15] Ran Canetti, Ari Trachtenberg, and Mayank Varia., "Anonymous collocation discovery: Taming the coronavirus while preserving privacy.," *arXiv e-prints, page arXiv:2003.13670, March 2020.*.

[16] "Apple Corona SDK," [Online]. Available: https://www.apple.com/covid19/contacttracing. [Accessed 4 August 2020].

[17] "Android Corona SDK," [Online]. Available: https://www.google.com/covid19/exposurenotifications/. [Accessed 4 August 2020].

[18] "Government Singapore," [Online]. Available: https://www.gov.sg/article/pm-lee-hsien-loong-on-the-covid-19-situation-in-singapore-3-apr. [Accessed 4 August 2020].

[19] S. Prasso, "Everyone Has a Contact-Tracing App, and Nobody's Happy About It," *Bloomberg*, 21 05 2020.

[20] Camenisch, J., Haralambiev, K., Kohlweiss, M., Lapon, J., & Naessens, V. , "Structure preserving CCA secure encryption and applications.," *International Conference on the Theory and Application of Cryptology and Information Security. Springer, Berlin, Heidelberg, 2011.*