

Corona-Warn-App: Tracing the Start of the Official COVID-19 Exposure Notification App for Germany

Jens Helge Reelfs
Brandenburg University of
Technology

Oliver Hohlfeld
Brandenburg University of
Technology

Ingmar Poesche
BENOCs

ABSTRACT

On June 16, 2020, Germany launched an open-source smartphone contact tracing app (“Corona-Warn-App”) to help tracing SARS-CoV-2 (coronavirus) infection chains. It uses a decentralized, privacy-preserving design based on the Exposure Notification APIs in which a centralized server is only used to distribute a list of keys of SARS-CoV-2 infected users that is fetched by the app once per day. Its success, however, depends on its adoption. In this poster, we characterize the early adoption of the app using Netflow traces captured directly at its hosting infrastructure. We show that the app generated traffic from all over Germany—already on the first day. We further observe that local COVID-19 outbreaks do not result in noticeable traffic increases.

CCS CONCEPTS

• **Networks** → **Network monitoring**; • **Information systems** → **Web applications**.

KEYWORDS

COVID-19, Contact Tracing, Exposure Notification

ACM Reference Format:

Jens Helge Reelfs, Oliver Hohlfeld, and Ingmar Poesche. 2020. Corona-Warn-App: Tracing the Start of the Official COVID-19 Exposure Notification App for Germany. In *ACM Special Interest Group on Data Communication (SIGCOMM ’20 Demos and Posters)*, August 10–14, 2020, Virtual Event, USA. ACM, New York, NY, USA, 3 pages. <https://doi.org/10.1145/3405837.3411378>

1 INTRODUCTION: CORONA-WARN-APP

The Corona-Warn-App [4] (CWA) is Germany’s official contract tracing smartphone app released on June 16, 2020. It aims to trace infection chains by informing users that were exposed to a person later tested positive. Centralized contact *tracking* by apps that report contacts to a central infrastructure raise privacy concerns, which is why a decentralized and privacy-preserving contract *tracing* approach (DP-3T) has been proposed [17]. This concept evolved to the Exposure Notification APIs by Apple [1] and Google [2], of which security and privacy properties were assessed [10]. The CWA uses the decentralized Exposure Notification approach to detect the proximity of other CWA users by collecting pseudonymous identifiers sent via Bluetooth Low Energy, only stored on the phone. Its

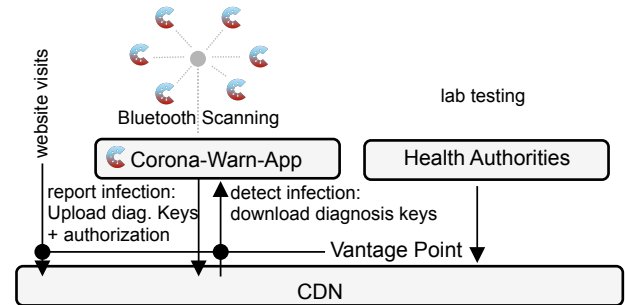


Figure 1: CWA architecture and vantage point

source code—including the Android and iOS smartphone apps, the backend server, and documentation—is released via Github [6].

We show the overall architecture including our vantage point in Figure 1. Phones locally store these received identifiers for 14 days. To protect the user’s privacy, all identifiers are volatile by generating new temporary exposure keys every 24 hours. If diagnosed with COVID-19, a user *can* decide to inform others by uploading (parts of her) temporary keys (diagnosis keys) used within 14 days to a central server, verified by health authorities. By monitoring the API, we observe the first diagnosis keys to be available on June 23 [3]. The CWA regularly downloads shared diagnosis keys from the central server, matches them against the local Bluetooth encounter history, and informs the user of having been exposed to an infected person within the past 14 days if keys match. Shared keys are non-personal identifiable and all contact tracing data never leaves the phone.

Goal. Since widespread adoption is key to the app’s success [14], we take the rare opportunity to monitor its nation-wide adoption starting at day 1. We measure *interest* in the CWA by monitoring CWA app and website traffic at its hosting infrastructure, enabling us to provide first insights into the adoption across Germany. We further study whether local COVID-19 outbreaks manifest in higher use.

2 DATA SET

We obtained sampled Netflow traces from routers connecting the data center hosting the CWA backend (see CDN in Figure 1). These flows contain web site visits *and* diagnosis key downloads by the app. All client IP addresses are prefix-preserving anonymized. We filter server traffic using 2 IPv4 prefixes mentioned in the CWA backend documentation [7] and omit IPv6. We verified their usage by resolving the API and web site DNS names (obtained from the app source code) against 10k open DNS resolvers from public-dns.info. As both, app and website, use HTTPS only, we restrict the data to encrypted HTTPS (tcp/443) IPv4 flows from the CDN to the user—resulting in $\approx 3.3M$ matching flows within June 15–25, 2020. **Limitations.** Website visits and CWA app API calls are served by the same servers via HTTPS and cannot be differentiated. The routers Netflow cache eviction settings and sampling result in only

Permission to make digital or hard copies of part or all of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for third-party components of this work must be honored. For all other uses, contact the owner/author(s).

SIGCOMM ’20 Demos and Posters, August 10–14, 2020, Virtual Event, USA

© 2020 Copyright held by the owner/author(s).

ACM ISBN 978-1-4503-8048-5/20/08.

<https://doi.org/10.1145/3405837.3411378>

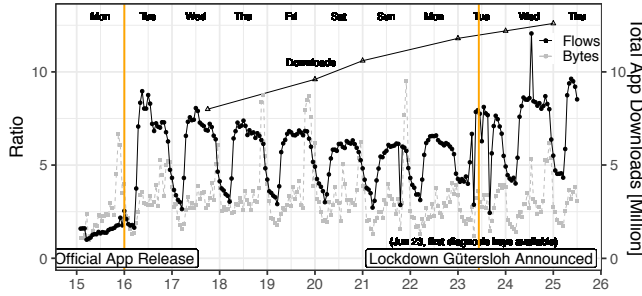


Figure 2: Hourly aggregated HTTPS traffic from CWA CDN to users normed to the minimum (left y-axis) and the total app downloads in million from Google/Apple (right y-axis).

observing few packets for most flows, making a flow-size based differentiation infeasible. While CWA should periodically download diagnosis keys, energy saving settings prohibit background downloads on some Android and iOS phones, reported on July 24 [5, 8] and to be fixed after our study. Periodic request pattern by CWA might thus be used in future work for app identification. Yet, the CWA API DNS name appeared in the Umbrella Top 1M domains [16] on June 24, 27, July 8, 10–11, while the website never appeared—implying *CWA API calls to be more popular than website visits* in OpenDNS and thus *might* dominate the #flows. Flows reveal trends in the interest in CWA and geolocation of destination routers/prefixes enables to study geographic adoption—the scope of this work.

Ethics. The Netflow data provides only flow summaries based on the packet header and does not reveal any payload information. All IP addresses are anonymized; it enables us analyzing aggregates of traffic flows between routers (to identify city-level location information of users) but not individual users. The flow-level statistics do not enable detecting infected users nor deriving any user-related information. Our analyses provide aggregated perspectives on the general interest in the app without compromising users’ privacy.

3 CWA APP: EARLY ADOPTION RESULTS

Temporal adoption. We show all HTTPS traffic from the CWA CDN to its clients in Figure 2 (flows and bytes normed to the minimum). It also cumulative shows officially reported downloads from the Apple and Google playstores [9], starting on June 17; 36 hours after its release, the CWA was downloaded 6.4M times (16.2M total downloads by July 24). With the official release of the CWA on June 16, the traffic immediately increases (7.5x increase of flows on June 16). Interest starts to follow the normal diurnal traffic pattern. After an initial steep traffic increase, it is reduced after a few days, just to re-surge when news in Germany started reporting higher infection rates again and subsequent lockdowns in two districts on June 23 [13] (Gütersloh and Warendorf) followed—widely covered in media.

By knowing that customers of certain ISPs keep the same IP address over time, we studied how regular routing prefixes communicate with the CWA backend (fraction of individual first to last day observed). We observe sustained interest as 50% (75%) of the prefixes occur in 67% (80%) of possible days.

Quick nation-wide spread. The success of the CWA app to trace infection chains by contact tracing depends on its adoption and geographic spread. We thus geolocate the request traffic (again both website requests and app API calls—both reflecting interest) within Germany shown in Figure 3 by ZIP code areas summed over 10

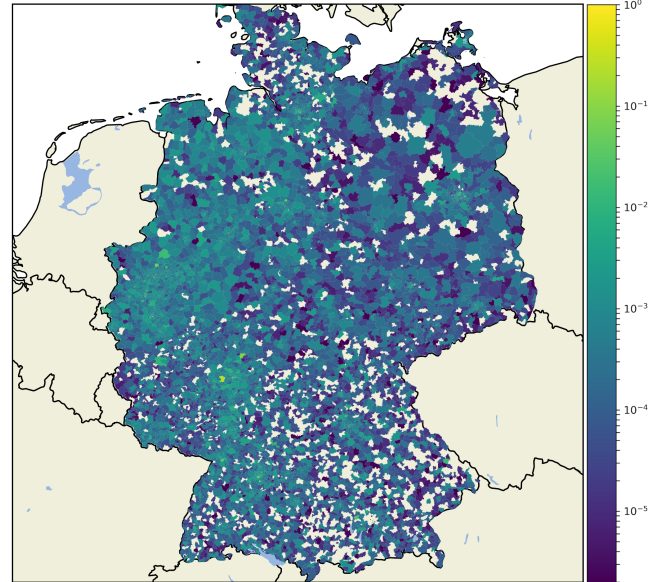


Figure 3: CWA traffic by district: usage across Germany aggregated over 10 days normalized by maximum

days. We derive 18% of geolocations from local routers within an ISP that connect customers (ground truth since the router locations are known), while the rest is located by applying the Maxmind geolocation database on routing prefixes. Note that client geolocation *can* be subject to errors; the router city-location can be off the clients location (e.g., in rural areas) and Maxmind’s geolocation can also be subject to inaccuracies at city-level [15]. We observe that almost all districts (shown in the heatmap by ZIP code areas) emit requests to the CWA backend. Notably, evaluating the geographic spread on the first day of the app leads to almost the same observation (not shown). In conclusion, the CWA triggered interest across a almost *all* German districts.

No effect of local COVID-19 outbreaks. Our measurement period contains two local COVID-19 outbreaks: *i*) in Berlin on June 18 [11], and *ii*) in Gütersloh and Warendorf on June 23 [13]. The latter (June 23) led to few domestic travel restrictions for visitors from these districts [12]. While we observe an increase in usage starting on June 23 (see Figure 2), this traffic increase also occurs on federal state level simultaneously—not only in the federal state (NRW) being home to the affected districts. In Gütersloh, the traffic increased only very slightly and hardly noticeable (insufficient data for Warendorf). The outbreak in Berlin on June 18 is only visible for users of a single ISP and not in the overall traffic from Berlin-based users. For now, we thus conclude that local COVID-19 outbreaks do not appear to generally increase traffic in only the affected regions. Instead, nation-wide news reports on outbreaks *might* contribute to growing app interest across Germany—an effect we aim to investigate in future work.

Conclusion. Already on its first day, the CWA app generated substantial interest—manifested in traffic from almost all German districts. Local COVID-19 outbreaks do not appear to increase traffic in the affected regions but can correlate to nation-wide increases. On this basis, we will investigate patterns driving local adoption in future work; e.g., if and how does news media fire CWA interest; and what will be the long-term app interest.

REFERENCES

- [1] [n.d.]. <https://developer.apple.com/documentation/exposurenotification>.
- [2] [n.d.]. <https://www.google.com/covid19/exposurenotifications/>.
- [3] [n.d.]. <https://github.com/ohohlfeld/corona-warn-app-monitor>.
- [4] 2020. Corona Warn App. <https://www.coronawarn.app/en/>.
- [5] 2020. Corona Warn App FAQ: My risk status hasn't been updated for over a day. An internet connection was available, what's wrong? <https://www.coronawarn.app/en/faq/>.
- [6] 2020. Corona Warn App Github. <https://github.com/corona-warn-app>.
- [7] 2020. German Corona Warn App (CWA) Backend Infrastructure Overview. <https://github.com/corona-warn-app/cwa-documentation/blob/master/backend-infrastructure-architecture.pdf>.
- [8] 2020. Germany's coronavirus tracing app initially 'disabled' on Android smartphones. <https://p.dw.com/p/3frEh>.
- [9] 2020. statista: Anzahl der Downloads der Corona-Warn-App Äijber den Apple App Store und den Google Play Store in Deutschland im Juli 2020. <https://de.statista.com/statistik/daten/studie/1125951/umfrage/downloads-der-corona-warn-app/>.
- [10] Lars BaumgÄdrtnr, Alexandra Dmitrienko, Bernd Freisleben, Alexander Gruler, Jonas HÄuchst, Joshua KÄijhlberg, Mira Mezini, Markus Miettinen, Anel Muhamedagic, Thien Duc Nguyen, Alvar Penning, Dermot Frederik Pustelnik, Philipp Roos, Ahmad-Reza Sadeghi, Michael Schwarz, and Christian Uhl. 2020. Mind the GAP: Security & Privacy Risks of Contact Tracing Apps. arXiv cs.CR/2006.05914 <https://arxiv.org/abs/2006.05914>.
- [11] Deutsche Welle. 2020. Berlin-NeukÄülln: Low income and migrant families in coronavirus lockdown. <https://p.dw.com/p/3e0Cd>.
- [12] Deutsche Welle. 2020. Germany maps out coronavirus regulations on domestic travel. <https://p.dw.com/p/3eQL4>.
- [13] Deutsche Welle. 2020. Germany puts two western districts on lockdown. <https://p.dw.com/p/3eEdt>.
- [14] Luca Ferretti, Chris Wymant, Michelle Kendall, Lele Zhao, Anel Nurtay, Lucie Abeler-Dörner, Michael Parker, David Bonsall, and Christophe Fraser. 2020. Quantifying SARS-CoV-2 transmission suggests epidemic control with digital contact tracing. *Science* 368, 6491 (2020). <https://doi.org/10.1126/science.abb6936>.
- [15] Ingmar Poesse, Steve Uhlig, Mohamed Ali Kaafar, Benoit Donnet, and Bamba Gueye. 2011. IP Geolocation Databases: Unreliable? *SIGCOMM Comput. Commun. Rev.* 41, 2 (April 2011), 53Ä56. <https://doi.org/10.1145/1971162.1971171>.
- [16] Quirin Scheitle, Oliver Hohlfeld, Julien Gamba, Jonas Jelten, Torsten Zimmermann, Stephen D. Strowes, and Narseo Vallina-Rodriguez. 2018. A Long Way to the Top: Significance, Structure, and Stability of Internet Top Lists. In *ACM Internet Measurements Conference*. 478Ä493. <https://doi.org/10.1145/3278532.3278574>.
- [17] Carmela Troncoso, Mathias Payer, Jean-Pierre Hubaux, Marcel SalathÄI, James Larus, Edouard Bugnion, Wouter Lueks, Theresa Stadler, Apostolos Pyrgelis, Daniele Antonoli, Ludovic Barman, Sylvain Chatel, Kenneth Paterson, Srdjan ÄNapkun, David Basin, Jan Beutel, Dennis Jackson, Marc Roeschlin, Patrick Leu, Bart Preneel, Nigel Smart, Aysajan Abidin, Seda GÄijrses, Michael Veale, Cas Cremers, Michael Backes, Nils Ole Tippenhauer, Reuben Binns, Ciro Cattuto, Alain Barrat, Dario Fiore, Manuel Barbosa, Rui Oliveira, and JosÄI Pereira. 2020. Decentralized Privacy-Preserving Proximity Tracing. arXiv cs.CR/2005.12273 <https://arxiv.org/abs/2005.12273>.