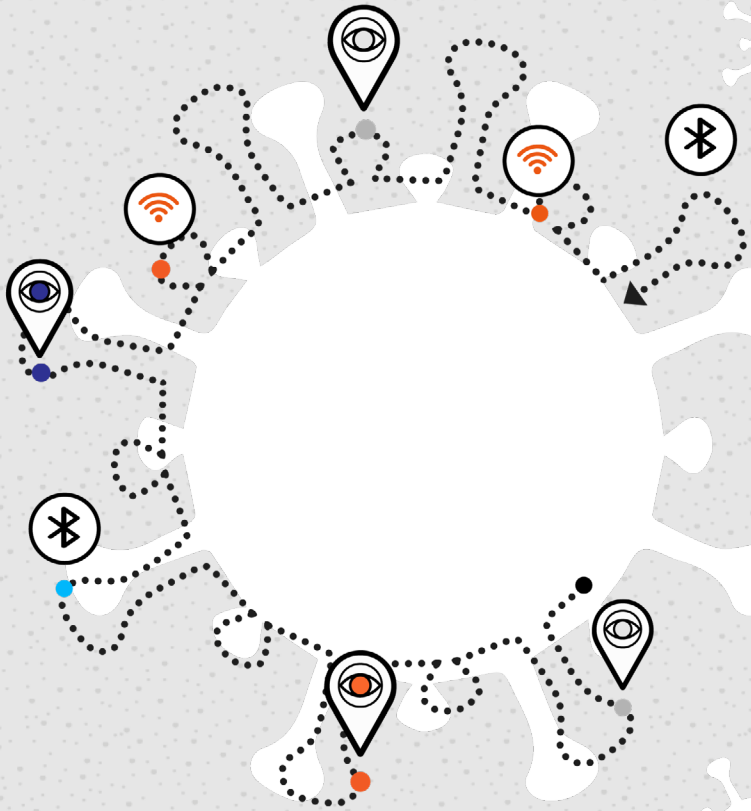
COVID-19 CONTACT TRACING APPS IN THE EU: LESSONS FROM GERMANY

#trackthetrackers



July 2021

CIVIL LIBERTIES UNION FOR EUROPE

Publisher
Civil Liberties Union for Europe e.V
Ringbahnstraße 16-18-20
12099 Berlin, Germany
www.liberties.eu

Author
Christian Thönnes

Editor
Orsolya Reich

Copy Editor
Jonathan Day

This study is part of the Civil Liberties Union for Europe's *COVID-19 Contact Tracing Apps in the EU* project. In the framework of this project, experts and civil society actors in ten EU Member States pursue research on the potentially concerning aspects of their national contact tracing apps. While said experts and civil society actors and the Civil Liberties Union for Europe generally stand for the same values, their views may not agree on all matters herein.

The *COVID-19 Contact Tracing Apps in the EU* project has been supported by the European AI Fund, a collaborative initiative of the Network of European Foundations (NEF). The sole responsibility for the project lies with the organiser(s) and the content may not necessarily reflect the positions of the European AI Fund, NEF or the European AI Fund's Partner Foundations.

Table of contents

Introduction

At the time of writing this report, Germany appears to be poised for a relatively calm summer. With only 6 active cases per 100,000 inhabitants on 25 June 2021, the third wave appears to have flattened in Germany.[1] Germany has also made good progress in its vaccination efforts: As of 25 June 2021, 34.8% of the German population is fully vaccinated against COVID-19, and 53.3% has received one dose.[2] This state of relative calm allows for a moment of reflection and analysis.[3]

This report aims to provide an analysis of the German deployment of contact tracing apps and at extracting some tentative lessons. These lessons, to be found at the end of this study, could provide some guidance in the future to civil society stakeholders and policymakers in the development and critical assessment of state-sponsored, data-driven solutions for public crises.

Two lessons deserve to be emphasized at the outset. First, data protection law poses no hindrance to innovation or public safety. Despite all ill-considered diatribes, the Corona-Warn-App (CWA) has proven that data protection and data security do not stifle innovation. It is very much possible to develop data-driven solutions to public crises which both work well and respect privacy.

Second, an engaged and critical civil society is vital in ensuring healthy developments in the digital space. The discourse around tracing apps was a prime example of the inestimable value of open social debate. Many positive developments - be it the rejection of invasive GPS data, suggestions for meaningful updates to the CWA, or the exposure of the extent of the Luca App's security problems - would not have been possible without this degree of openness and commitment. The digital political community should maintain this high level of social vigilance for future digital policy debates. However, we should also become better in refuting the narrative that privacy undermines safety. We have to organize and convince a significant part of the general public of this, because if we fail to do so, the political pressure on decision makers to introduce unacceptable solutions will be too high.

1 https://de.statista.com/statistik/daten/studie/1192085/umfrage/coronainfektionen-covid-19-in-den-letzten-sieben-tagen-in-deutschland/.

2 https://impfdashboard.de/.

3 It is a "relative" calm as the so called "delta" variant may change the situation in the coming weeks.

Methods

Several experts were consulted in the creation of this report:

- ***Henning Tillmann.*** Mr. Tillmann holds a degree in computer science and is a self-employed software developer living in Berlin. He is co-chair of the digital policy think tank D64 - Center for Digital Progress.

- ***Dr. Malte Engeler.*** Mr. Engeler is a judge at the Administrative Court of Schleswig-Holstein and an expert in data protection law.

- ***Professor Viktor von Wyl.*** Mr. von Wyl holds a PhD in Epidemiology and is Assistant Professor for Digital and Mobile Health at the University of Zurich. He has co-published several studies on the effectiveness of the "SwissCovid app".

In addition, a number of freedom of information and press requests were submitted to German authorities, including the German Federal Ministry of Health, the Robert Koch Institute (RKI), the Federal Commissioner for Data Protection and Freedom of Information, as well as the Berlin Commissioner for Data Protection.

The rest of this report is based on desk research. Wherever scientific studies or other sources are referenced, they are quoted in footnotes.

Paradigms of responsible digital governance

During the past months of battling the COVID-19 pandemic, much has been said and written about tracing apps. Sometimes they were hailed as a quasi-panacea, sometimes dreaded as a surveillance nightmare and sometimes dismissed as effectively useless. The only undebated fact is that the deployment of contact tracing apps has been one of the main pillars of the German government's tech response to the pandemic.

In order to be able to critically assess the German tech response to the pandemic, it is important to come up with a normative framework, against which tracing apps can be compared. The following principles represent an aggregation of the recommendations which were made by the World Health Organization and numerous independent expert groups.[4]

- **Transparent open-source solutions:** When governments develop software, they should pursue a strictly open-source strategy. When purchasing software from private manufacturers, governments should insist that the software's source code be released. Only then can independent experts identify security loopholes and other flaws early on so that privacy and security by design can be achieved. Moreover, data-driven solutions can only unfold their full potential when they are met with broad social acceptance. And that acceptance can only be achieved when all people affected know what they are consenting to.

- **Prioritization of decentralized solutions:** Whenever possible, governments should opt for decentralized data storage structures. Experience has shown that, when large data treasures fall into the hands of powerful central entities, often numerous human rights and security breaches ensue. Under modern technological circumstances, putting large amounts of sensitive data into the hands of just one central entity means transferring an amount of responsibility which is just too large to bear.

- **Voluntary use:** The installation and use of contact tracing apps should remain strictly

4 World Health Organization, Ethical considerations to guide the use of digital proximity tracking technologies for COVID-19 contact tracing principles; Chaos Computer Club, Prüfsteine für die Bewertung von Contact Tracing Apps; Contact tracing joint statement. Naturally, these principles are neither fully comprehensive, nor are they carved in stone. To a large extent, this selection reflects the author's limited perspective and policy preferences. With new challenges and rapidly evolving technological possibilities, some principles may themselves evolve or be replaced by other ones.

voluntary. True voluntariness means freedom from both direct obligation and indirect coercion (e.g. through tax incentives, insurance premiums, denial of access to public transport or other resources etc.).

- **Adequate security measures:** Industry best practice standards should be adopted in order to mitigate the risk of intrusions, data breaches and other security issues. Among other measures, this includes modern encryption technology.

- **Accountability:** Data controllers and manufactures should not close themselves off from public debate but should take every reasonable measure to facilitate public debate about the quality and security of the software in use. One suitable step towards accountability is to release a data protection impact assessment (Article 35 GDPR) to the public.

- **Compliance with established data protection law standards:** There is no such thing as a state of data protection emergency where security generally trumps freedom from surveillance. All main tenets of data protection law – among others the principles of proportionality (Recital 170 GDPR), purpose limitation (Art. 5 § 1 letter b GDPR), data minimization (Art. 5 § 1 letter c GDPR), data security (Art. 5 § 1 letter f GDPR) and privacy by design (Art. 25) – still apply in times of emergency. Pressing public needs may justify a higher degree of data processing. But these measures must always be strictly limited to what is necessary to achieve a public end. Data processing must be strictly limited to the public end for which it was originally intended; governments must resist the temptation of giving in to law enforcement authorities who come knocking at their door asking for access. Privacy threats must be mitigated as far as possible, for example through strong encryption. On that note, when data collection is increased in times of emergency, there should always be a pre-defined "exit plan". All processing must cease and all personal data must be deleted once the public threat has passed.

- **Independent oversight:** Data protection authorities must critically assess data-driven solutions. In so doing, they must fulfill their mission of independent supervision without giving in to political pressure for the sake of maintaining the appearance of being "open to innovation".

- **Constant monitoring, updates, and evaluation:** After a piece of software has been released, the government's job is far from over. Instead, responsible governments must ensure that apps are constantly monitored for potential security loopholes. Where necessary, additional functionalities must be implemented as soon as possible. Governments must create responsible bodies capable of fulfilling these tasks. Moreover, tech responses should be evaluated through independent and well-financed research. If the solution turns out to be ineffective, it must be adjusted or terminated.

- **Avoidance of digital hubris:** Claiming to solve problems "through innovation" may easily garner political popularity. While technologies are sometimes useful additions,

they are rarely a complete substitute for a well-rounded governance strategy. Applied to the pandemic response, this means that contact tracing apps can be one tool among many. Pretending like they are a panacea, making all other containment strategies, like social distancing or wearing face masks, obsolete, would only result in unreasonable and excessive expectations which will inadvertently be frustrated – only to then turn into declining social trust and finger-pointing at fundamental rights like data protection.

Tracing apps in practice – The German tech response during the first, second and third pandemic wave

During the summer of 2020, Germany was widely praised for its pandemic response.[5] During the first wave, lasting roughly from March to June of 2020, Germany had managed to flatten the proverbial curve quite efficiently. On 12 June 2020, the date of the *Corona-Warn-App's* (CWA) release, there were about 3 known COVID-19 cases per 100,000 inhabitants in Germany.[6]

For a long time, Germany's status as an efficient pandemic policymaker was not limited to the virus's general containment. It also extended to its perceived proficiency in digital policy. At least until the second wave arrived, most digital policy experts lauded the German government's development and deployment of the CWA as a rare-yet-welcome example of responsible digital policy.

This status, however, waned with the perceived quality of Germany's broader pandemic response. As new waves of infection cases arrived, trust in the government's handling of the pandemic declined and policymakers came under pressure. This development had a significant impact on Germany's tech response.

The debate around tracing apps was thus transformed as pandemic waves came and went. To highlight this change, it appears useful to retell and analyse the German tech response through the pandemic's main phases:

Tracing apps during and after the first wave – Off to a good start?

Initial plans

The idea of tracing apps arose very early in German public debates on how to fight the coronavirus pandemic. Technology enthusiasts advocated that digital contact tracing could increase the chances of tracing risk contacts potentially exposed to an infection, warn those contacts very early and thus make it more likely that these exposed contacts would self-quarantine before they could infect others. Digital contact tracing, it was believed,

5 New York Times, A German Exception? Why the Country's Coronavirus Death Rate Is Low.

6 https://de.statista.com/statistik/daten/studie/1192085/umfrage/coronainfektionen-covid-19-in-den-letzten-sieben-tagen-in-deutschland/.

could represent a milder alternative to strict lockdown measures.

At first – not unusually for German security discourse – draconian surveillance measures were proposed as an approach to contact tracing. The Federal Ministry for Health originally proposed to oblige providers of telecommunications services to share location and movement (so most likely GPS) data with health authorities.[7] After much public criticism, however, this passage was withdrawn and did not make it into passed amendments to the Infection Protection Act (*Infektionsschutzgesetz*).

It then appeared clear that public authorities would make use of Bluetooth Low Energy (BLE) technology instead of resorting to GPS. This was a sound decision, since GPS would at the same time be much more invasive and much less useful in identifying risk contacts than BLE – whether you were coughed on at the bus stop or at home is completely irrelevant for identifying a risk of infection.

The main subject of public debate then became the choice between centralized and decentralized solutions. The first standard which popped up in the German debate was developed by the European consortium Pan-European Privacy-Preserving Proximity Tracing (PEPP-PT). Jens Spahn, the German Federal Minister of Health, initially favored the PEPP-PT standard.[8] While being open-source, it would have required personal data to be stored in a centralized database. This led a group consisting of 300 academics and numerous organizations, including the Chaos Computer Club (CCC), D64e.V., the Foundation for Data Protection (*Stiftung Datenschutz*) and many more, to publish open letters advocating against the PEPP-PT standard and for a decentralized approach[9] – a stellar example of civil society engagement.

The Google/Apple Exposure Notification (GAEN) system

Proponents of a decentralized system pointed to an alternative standard: Decentralized Privacy-Preserving Proximity Tracing (DP-3T). Shortly after, Apple and Google teamed up to develop the "Google/Apple Exposure Notification" framework (GAEN).[10] GAEN is an application programming interface (API) which is necessary to have contact tracing apps perform BLE operations smoothly in the background on a smartphone. Apple's iOS usually prevents third-party apps from broadcasting Bluetooth signals from the background. This means that, without access to the GAEN API,

7 The draft can be accessed here.

8 Handelsblatt, Spahn entscheidet sich für umstrittenes Corona-App-Modell.

9 Offener Brief zu Kontaktverfolgungs-Apps beim Coronavirus, accessible via: https://www.sciencemediacenter.de/alle-angebote/rapid-reaction/details/news/offener-brief-zu-kontaktverfolgungs-apps-beim-coronavirus/; https://www.ccc.de/system/uploads/300/original/Offener_Brief_Corona_App_BMG.pdf

10 https://covid19.apple.com/contacttracing.

users would either constantly have to keep the contact tracing app open – which means keeping their phone unlocked, risking third-party intrusion and quick battery drainage – or experience low-quality performance.

In order for a national contact tracing app to gain access to GAEN, the respective government must make a request to Google and Apple. Google and Apple decided to only grant access to decentralized app architectures (similar to the DP-3T standard) which use encryption in order to avoid revealing users' identities. This was highlighted by the fact that they denied the French tracing app *StopCovid*, which pursued a centralized approach, access to GAEN.[11]

The Corona-Warn-App

After German officials failed to convince Apple and Google to grant a PEPP-PT-based app access to GAEN, the German government decided to change course and opt for a decentralized, DP-3T approach.[12] The Federal Ministry of Health and the RKI commissioned SAP and Deutsche Telekom with developing a contact tracing app – and born was the plan for the *Corona-Warn-App*.

The CWA's installation and use is voluntary. It uses Bluetooth Low Energy (BLE) technology to log encounters on an anonymous contact diary. Registration or personal information is not required to install the app. Once installed, the app generates a random key, which is updated every day. This daily key is not shared with other devices. Instead, every 10 to 20 minutes, an RPI (Rolling Proximity Identifier) is generated. The RPI, a shorter key, is derived from the daily key – knowing the daily key enables you to infer RPIs, but knowing RPIs alone does not enable you to infer the daily key. When two devices are in such proximity to each other that they register the exceeding of a certain signal threshold – which is usually defined as being within 1.5 meters of each other for a period of at least 10 minutes – two devices exchange their current RPIs. These RPIs are only stored locally on the respective devices for a period of 14 days. Contrary to what occurs in a centralized system, the RPIs are not automatically transferred to a central server.

When a user tests positive for COVID-19, they can voluntarily decide to register their test results via the app and thus trigger warnings for their contacts. Provided that the testing laboratory is already integrated into the app's system, users will receive a QR code upon taking a (usually PCR) test. In that case, when users scan the QR code via the app, they receive a verified test result which they can then share. If, however, the respective testing laboratory is not yet connected to the app's system, users can verify and thus integrate their test results by calling a telephone hotline where they receive a teleTAN.

11 BBC News, Coronavirus: Apple and France in stand-off over contact-tracing app.

12 Reuters, Germany flips to Apple-Google approach on smartphone contact tracing.

When a verified positive test result is shared, the device's daily keys of the last few days are transmitted to the CWA's server. This server is controlled by the RKI. All app users' devices regularly connect to the CWA's server in order to download all daily keys, which are marked as belonging to users who were tested positive for COVID-19. These downloaded positive daily keys are processed in the GAEN API, where all possible RPIs are generated from the received positive daily keys. These RPIs are then matched with all locally stores RPIs which were received due to the above-described degree of proximity.

For all identified matches, the GAEN framework then calculates an infection risk score. This is done by determining the duration of the encounter, estimating the proximity of the infected person based on the signal strength of the Bluetooth signal, taking into account the transmission risk of the infected person from tag data included in the daily key and the time span since contact. Before the calculation, current configuration data are downloaded from the CWA server. These configuration data contain weighting factors for all relevant parameters.[13]

The risk score results in three possible messages which are displayed to app users on the CWA's interface:

- **Increased risk (red):** Users are asked to self-quarantine and contact medical professionals via telephone in order to get tested and/or receive treatment if they suffer from symptoms.

- **Low risk (green):** Users are asked to comply with the usual hygiene standards.

- **Unknown risk (white):** Displayed when the app has not been operating for a sufficient amount of time or when technical problems occurred.

Compliance with data protection and safety standards

Independent IT experts – among others, the *Chaos Computer Club*, which is usually highly skeptical of governmental IT projects – reviewed the source code and found no significant data security or privacy risks. A detailed data protection impact assessment (Art. 35 GDPR) for the CWA was released.[14] The CWA was developed in close cooperation with the German Federal Commissioner for Data Protection and Freedom of Information (BfDI), Prof. Ulrich Kelber, who supported the CWA from the start. Until this day, at least according to public knowledge, the CWA has suffered from no significant data breaches or other security problems. To a freedom of information request (FOI), the BfDI

13 For an in-depth description of the CWA's technical details, refer to pages 17-117 of the current DPIA (see note 13).

14 Corona-Warn-App, Bericht zur Datenschutz-Folgenabschätzung für die Corona-Warn-App der Bundesrepublik Deutschland, öffentliche Version, current version: 1.12 from 11 May 2021 (in following notes: CWA DPIA).

responded that they received 122 data protection complaints. So far, these complaints have not led to any widely-reported-on or scandalous investigations.

In the course of the CWA's release, a debate sparked around the adequate legal basis for its processing of personal data. Even with the strongest encryption, when positively tested daily keys are transferred to the CWA's server, they come with the device's IP address; IP addresses are personal data because they allow the transmitted information to be traced back to the origin device's user.[15] This means that even in the decentralized app system, personal data – potentially even especially sensitive health data (Art. 9 § 1 GDPR) – are processed by the RKI, a government entity.[16] For this processing, a legal basis is required (Art. 6 § 1, Art. 9 § 2 GDPR).

The RKI considers consent (Art. 6 § 1 letter a; Art. 9 § 2 letter a GDPR) to be an appropriate legal basis.[17] There is reason to believe, however, that consent does not constitute a sufficient legal basis. It is for this reason that civil society actors, such as a group of legal experts led by Dr. Malte Engeler and the Gesellschaft für Freiheitsrechte, advocated for a formal legal basis for the app's usage, in accordance with Art. 6 § 1 letter e, Art. 9 § 2 letter g GDPR.[18] This legal basis should have, in their opinion, explicitly prohibited state and powerful private actors from tying punitive measures (such as tax or insurance penalties, denials of access to public places and transportation or penalties in labor law) to non-usage of the app.

"The GDPR stipulates that there is such a power imbalance in the relationship between the state and the individual that citizens usually cannot consent to processing in a truly voluntary fashion. This becomes clear from recital 43 of the GDPR," Dr. Engeler argues. "The CWA is run by the RKI, a government entity - so consent just doesn't come voluntarily."

Dr. Engeler's arguments fell on deaf ears. To this day, Germany has not created a legal basis for the CWA. This stands in contrast to other countries like Switzerland, which have created legal bases for their contact tracing apps.[19] He says: "These legal arguments were probably difficult to convey in this complex political situation. Nevertheless, it irritates me that the BfDI never took action here. BfDI must know that consent is not a suitable legal basis for the CWA."

15 European Court of Justice, Judgment of the Court, 19 October 2016, C-582/14, „Breyer".

16 The CWA DPIA concedes this on pages 119 and following.

17 CWA DPIA, pages 129 and following.

18 Mr. Engeler published a draft law which can be accessed here.

19 See Art. 60a of the Swiss "Bundesgesetz über die Bekämpfung übertragbarer Krankheiten" (Federal Law on the Control of Infectious Diseases), entitled "Proximity-Tracing-System für das Coronavirus" (Proximity Tracing System for the coronavirus).

As the RKI states on page 136 of their DPIA's current version, there is no publicly available indication suggesting that state or powerful private actors have exerted direct or indirect pressure which would have rendered the CWA's use *de facto* mandatory. A response by the Berlin Commissioner for Data Protection to an FOI request points in the same direction: In replying to our respective questions, they confirm that they have received no complaint which would suggest otherwise.

This does not, however, make the initial legal assessment that a legal basis would be required, redundant or false. It just means that choosing a potentially inadequate legal basis did not yield severe consequences.

Tracing apps during the second wave – Peculiar inaction

Throughout the summer of 2020, user numbers for the CWA were steadily rising. By September, roughly 18 million people had downloaded the app.[20] This is equivalent to about 22% of the German population. During this period of prolonged epidemic calm, many experts were already warning of a second wave. Indeed, August and September had seen a slight uptick in infection numbers: On 3 August 2020, there were 5.1 infections per 100,000 inhabitants. On 28 September, one could already observe a tendency towards exponential growth with 14 per 100,000. Infection rates indeed exploded in October 2020. By 9 November, there were already 139 infections per 100,000 inhabitants. [21]

Proposals for updates

Many experts proposed updates to the CWA's functionalities so that digital contact tracing could become an even more effective tool in combatting an impending second wave. Prominent amongst these voices has been Henning Tillmann. In an op-ed, published in German weekly newspaper DIE ZEIT on 1 September 2020, Henning Tillmann, along with Members of the German Parliament and epidemiological expert Karl Lauterbach, called for numerous updates to the CWA.[22] Among other ideas, they presented a concept for automatic cluster recognition.

Cluster recognition was chief among the functionalities demanded by epidemiological experts. These experts pointed to new scientific insights into the corona-virus's dissemination dynamics. Recent studies had demonstrated that one of the main accelerators of the virus's spread were so-called "superspreader events",

20 https://de.statista.com/statistik/daten/studie/1125951/umfrage/downloads-der-corona-warn-app/.

21 https://de.statista.com/statistik/daten/studie/1192085/umfrage/coronainfektionen-covid-19-in-den-letzten-sieben-tagen-in deutschland/#:~:text=Bis%20zum%2018.,10%20F%C3%A4lle%20je%20100.000%20Einwohner.

22 Die ZEIT, Vier Upgrades, die die Corona-Warn-App jetzt braucht.

meaning single events where, due to close proximity within a group, an infected person ends up infecting a large number of people.[23] Efficiently tackling these superspreader events through digital contact tracing would require the CWA to be capable of registering cluster risk events, rather than just individual infection chains.

Henning Tillmann's proposal for automatic cluster recognition would have entailed making use of other possible smartphone signals, such as Wifi signal receivers or pedometers. These signals could be used to enable a device not only to register individual contacts but its general surroundings. The device could thus expand its potential beyond only collecting daily keys according to the defined threshold for a risk contact. Instead, it could, for certain periods of time, register whether the device's user has been in movement or stationary, whether the device has been logged into a Wifi network (thus suggesting a risky indoor situation), and it could count for how long it has been in proximity to how many other devices emanating Bluetooth and Wifi search signals. This, way the CWA would enable the device to automatically recognize a potential cluster situation. In a case of a positive COVID-19 test, the CWA could then trigger warnings to all other devices which were part of the same cluster situation, regardless of whether the defined threshold for an individual risk contact has been crossed.

According to Henning Tillmann, this approach would not have required the exchange of particularly sensitive GPS data and it would have been compatible with the CWA's decentralized approach

Slow implementation of updates

The CWA did receive some updates during the second wave:

- Throughout the summer, half of Germany's testing laboratories remained unconnected to the CWA's system[24]. This required test recipients, instead of just scanning a QR code, to manually verify their test results. Empirical research has demonstrated that this test verification bottleneck drastically reduced the tracing app's capability to prevent infections.[25] By fall of 2020, 90% of German laboratories' testing capabilities had been integrated.[26]

- On 19 October 2020, the CWA was integrated into the European interoperability

23 This was emphasized by Germany's most prominent epidemiologist, Professor Christian Drosten in this op-ed: Die ZEIT, Ein Plan für den Herbst.

24 Ärztezeitung, 90 Prozent der Labore melden an Corona-Warn-App.

25 Von Wyl, Challenges for non-technical implementation of digital proximity tracing: early experiences from Switzerland, JMIR mHealth and uHealth doi: 10.2196/25345.

26 Robert-Koch-Institut, Kennzahlen zur Corona-Warn-App vom 12.10.2021.

gatewayservice, thus allowing it to interact with other European tracing apps.[27]

- Since December 2020, the app has a contact journal where users can note whom they have met in the last two weeks.[28]

- On 16 December 2020, the risk calculation method was improved.[29]

- In January 2021, the CWA received new functionalities, including statistics provided by the RKI on confirmed new infections, warnings by app users or the 7-day incidence rate.[30]

All throughout the second wave, however, the German government, along with SAP and Deutsche Telekom, failed to implement a cluster recognition or event registration feature.

Tracing apps during the third wave – Panic

Thus, Germany headed out of the second pandemic wave with a tracing app lacking a cluster recognition or event registration feature. And the calm before the third wave did not last all too long: While Germany managed to suppress their infection rates down from 167 per 100,000 on 11 January 2021 to 57 on 14 February, by 30 March they were up to 135 again, reaching their peak on 26 April with 169.[31]

In the eyes of many, this renewed explosion of infection rates – right after a period where the government had seemingly brought the pandemic spread back under control – revealed gross incompetence and flawed management on the government's part. During the early months of 2021, trust in the government's handling of the pandemic sharply declined.[32] Consequently, in this period, responsible policymakers were under a lot of pressure to do "something" to alleviate the situation of a populace under significant pandemic fatigue. This pressure was compounded by the fact that, with German federal parliamentary elections coming up in September 2021, many politicians started to shift into "campaigning mode".

A growing sentiment of political anxiety and frustration could be observed, among other things, in an anti-data protection narrative that was propagated by many politicians and

27 https://ec.europa.eu/commission/presscorner/detail/en/ip_20_1904.

28 https://github.com/corona-warn-app/cwa-app-android/releases/tag/v1.10.1.

29 https://github.com/corona-warn-app/cwa-app-ios/releases/tag/v1.9.1.

30 Tagesschau, Corona-Warn-App mit neuen Funktionen.

31 https://de.statista.com/statistik/daten/studie/1192085/umfrage/coronainfektionen-covid-19-in-den-letzten-sieben-tagen-in-deutschland/.

32 https://de.statista.com/statistik/daten/studie/1221212/umfrage/entwicklung-des-vertrauens-in-die-bundesregierung-waehrend-der-corona-krise/#professional.

journalists in late 2020 and early 2021. During these months, several op-eds and statements appeared, in which the CWA was described as a "toothless tiger"[33] (in this case by Bavarian Minister-President and then-contender for the CDU/CSU chancellor candidacy, Markus Söder) and where all-too-strict data protections standards were faulted for hampering the CWA and generally standing in the way of effectively containing the pandemic.[34]

This complicated situation created incentives for policymakers and governmental authorities – if they did not have anything actually useful to show – to simulate action and point fingers. The fact that Germany entered into this dynamic without a fully-fleshed-out CWA would later prove fatal for the German tech response.

The Luca App: Why it exists and how it works

This is the moment when the so-called "Luca app" (in the following paragraphs, just named "Luca") enters the stage. Luca promised to fill the gap that the CWA had left by failing to integrate a cluster recognition or event registration feature.

By the spring of 2021, most of the Bundesländer's SARS-CoV-2 Infection Protection Measures Ordinances ("Infektionsschutzverordnungen") required hosts of social gatherings (restaurant owners and so forth), to record their guests' personal data. This was done in order to put health authorities into the position to conduct manual contact tracing. Up until this point, the recording of personal data had been done manually, on physical slips of paper. This in turn opened room for all sorts of privacy abuses such as stalking by restaurant owners or data transfers to law enforcement. [35]

Therefore, Luca convinced many policymakers by offering to digitize the seemingly anachronistic manual contact recording process. "The main privacy problem Luca solved was preventing restaurant owners from gaining access to their guests' sensitive personal data," Henning Tillmann says. Its PR success was bolstered by the fact that Luca was promoted by Smudo, a member of the famous German hiphop group "Die Fantastischen Vier".

33 Bayerischer Rundfunk, Söder: Corona-Warn-App "bisher ein zahnloser Tiger".

34 Other articles making similar arguments: https://www.focus.de/politik/deutschland/schwarzer-kanal/die-focus-kolumne-von-jan-fleischhauer-ahnungslos-durch-die-krise-der-verhaengnisvollste-fehler-in-merkels-corona-politik_id_12631609.html; https://www.zeit.de/2021/01/corona-kontaktverfolgung-taiwan-suedkorea-app-datentechnologie; https://www.zeit.de/2021/21/thomas-de-maziere-corona-politik-macht-grundgesetz; for a summary of this debate and refutal of its central arguments: https://www.berliner-zeitung.de/wirtschaft-verantwortung/hemmt-der-datenschutz-die-pandemiebekaempfung-li.147271.

35 taz, Lust auf Liste.

In Luca, users can sign up with their name and contact details. These contact details are verified through a TAN which is sent via the user's registered cellphone number. Users can then scan a QR code whenever they are entering a restaurant or other event. Event hosts can generate these QR codes through the app. Alternatively, event hosts can scan guests' QR codes, which can be newly generated every minute. In any case, upon check-in guests' personal data are encrypted and stored centrally on the Luca team's servers.

According to the Luca team, personal data are encrypted twice: Once on each user's smartphone with the health authority's encryption key, and a second time upon check-in at an event location with the respective event host's key. This is intended to prevent both the Luca team and event hosts from being able to unilaterally gain access to unencrypted data.[36]

If a Luca app user tests positive for SARS-CoV-2, they can share their event attendance history with the health authority using a twelve-digit transaction number (TAN). Based on these data, the health authority then requests contact data for the affected event's attendees from the Luca team. The Luca interface then forwards this request to the respective event host via the Luca back-end. Event hosts can then release the requested contact data and decrypt them with their host encryption key. At this point, the contact data are still encrypted with the health authority's encryption key so that neither event hosts nor the Luca team can view the contact data in their unencrypted form. Upon receipt, health authorities can finally decrypt the contact data with their encryption key so that they – and only they – can view them in their unencrypted form.

It is then incumbent on the health authority to trigger a central warning to all affected users – note that this differs from the CWA's decentralized approach where affected users are warned directly upon submission of verified positive test results without any central government entity having to intervene. Thus, while the Luca app relies on the competence (and resources) of government authorities to compel users through binding legal force, the CWA relies on individual users' responsibility to comply with their duty to self-quarantine.

It is noted, however, that understanding how Luca works had at first been made difficult by the app's manufacturer: The source code was only released after relentless pressure by the online community. The release itself was beset with problems: At first, the manufacturer used an extremely restrictive license which forbade everyone from duplicating, sharing or otherwise reproducing the code on public networks – thus making critical analysis of the code practically impossible.[37] In defending Luca's reluctant approach to transparency, Luca CEO and

36 See Luca FAQs here: https://www.luca-app.de/faq/#ac_6921_collapse3.

37 Netzpolitik.org, Die fantastische Lizenz der Luca-App.

co-founder Patrick Hennig cited long-refuted notions of security through obscurity.[38]

Government authorities' concerning reaction to an inadequate piece of software

From the start, Luca was beset with technical problems and security breaches. It is hard to convey the degree of heated criticism and profound frustration that permeated discussions around Luca in the online community. Almost every week, there seemed to be a new flurry of deeply concerning problems and breaches occurring with Luca. Here are just some of the highlights:

- **Dissatisfying key management:** As criticized by the DSK,[39] all Luca encryption keys are centrally managed by the Luca app team. At least initially, all health authorities in Germany were provided with the same public encryption key. According to the DSK, "this poses the avoidable risk that a large number of the data which are centrally managed by the system can be accessed without authorization by spying on or misusing these keys. Likewise, it is difficult for hosts to verify whether a request for decryption is made legitimately, so they could be tricked into decrypting data without a legitimate request. A successful attack on the systems of culture4life GmbH can therefore put the security of the entire system at risk."[40] The DSK therefore asked the Luca team to investigate whether their app's functionalities could be implemented in a decentralized system.

- **Movement profiles through physical keyring pendants:** The Luca team offers physical keyring pendants, which are equipped with printed QR codes. This is supposed to allow to integrating people without modern smartphones into Luca's digital contact tracing. Under the hashtag "Lucatrack", a group of IT experts uncovered how third parties could make use of these physical keyring pendants in order to reconstruct movement profiles for individual users. Since, contrary to Luca's digital QR codes, the physical QR codes remain the same, a photo of them suffices to be capable to track all check-ins that were conducted throughout the past 30 days. After this revelation, Luca founder Patrick Hennig refused to take Luca's physical keyring pendants off the market, which numerous IT experts had urgently recommended.[41]

- **Code Injection through CSV files:** In May 2021 – more than two months after Luca's release – IT expert Marcus Mengs revealed

38 taz, Streit um Luca-App in Berlin.

39 Datenschutzkonferenz, Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder; in English: Data Protection Conference, Conference of Germany's Independent Data Protection Authorities. The DSK's statement on the Luca app can be accessed here.

40 DSK statement, p. 2-3.

41 netzpolitik.org, Schlüsselanhänger mit Folgen.

that Luca had a significant security gap which allowed hackers to infiltrate health authorities' IT systems with malware. The Luca team had neglected to disable the use of special characters (such as "=") in their name registration forms. This allowed users to program codes into CSV files. When health authorities open these CSV files with Microsoft Excel (and ignore a fairly standard security warning), a macro is executed. This way, contact data could be deleted or extracted from the health authority's system or ransomware could be installed. In a public statement, the Federal Office for Information Security ("Bundesamt für Sicherheit in der Informationstechnik", BSI) confirmed this security gap and said that the Luca team was responsible for it.[42] Linus Neuman from the CCC as well as Marcus Mengs noted that the Luca team had been warned against security problems numerous times prior before this particular incidence and that they had reacted with denials every time.[43]

These and numerous other security problems led many experts to speak out: 70 leading German IT security researchers published an open letter in which they sharply criticized Luca and strongly warned against its purchase and use.[44] In the letter, they wrote that Luca fulfilled none of the four main tenets of responsible contact tracing apps: purpose limitation, transparency, voluntariness and proportionality. The CCC demanded a "federal emergency break" ("Bundesnotbremse") for Luca.[45]

Henning Tillmann says: "Luca's vulnerabilities with physical keyring pendants and CSV files should not have happened. These problems could and should have been identified and fixed in advance."

Moreover, to this day, the Luca team has not publicized a DPIA. Article 35 of the GDPR includes no obligation to make DPIAs public, but not doing so does not speak well for Luca's commitment to transparency. In addition, it does appear that the competent data protection authorities were not provided with Luca's DPIA, which would be a breach of the GDPR. Notably, on 6 April, the Berlin Commissioner for Data Protection replied to an FOI that they had not received Luca's DPIA, yet.[46] To this, Malte Engeler says: "DPIAs must be in place from the start. If data protection authorities are willing to waive this legal obligation, one wonders what other data protection requirements are treated as dispositive."

All these concerns did not prevent most German federated states from purchasing licenses for Luca. By 12 April 2021, 13 out of the 16 federated states, namely Mecklenburg-Vorpommern, Berlin, Lower Saxony, Hesse,

42 https://twitter.com/BSI_Bund/status/1398195272400920578.

43 Die ZEIT, Hacker können Gesundheitsämter über Luca angreifen.

44 Gemeinsame Stellungnahme zur digitalen Kontaktverfolgung.

45 Die ZEIT, Hacker können Gesundheitsämter über Luca angreifen.

46 Gemeinsame Stellungnahme zur digitalen Kontaktverfolgung.

Rhineland-Palatinate, Bremen, Baden-Württemberg, Schleswig-Holstein, Saarland, Bavaria, Saxony-Anhalt and Hamburg, had purchased such a license for a combined sum of more than 20 million euros.[47] During spring, most of these federated states changed their Infection Protection Measures Ordinances specifically to allow for the manual contact data registration to be replaced with Luca.

Potentially even more concerning is the role played by data protection authorities. The Data Protection Commissioner of Baden-Württemberg played a particularly dubious role. In a press statement on 17 February 2021, he lauded Luca and recommended its use: "The app meets our high data protection standards. The documentation of the contacts is encrypted to the highest technical standard and it is solely up to the Luca user whether, when and with whom he or she wishes to share this sensitive data."[48] He later stated that he made these recommendations without having access to Luca's source code.[49] He reiterated his stance in an in-depth statement in March 2021[50] and he never retracted his initial stance on Luca despite the continuous disclosure of one security breach after another, even reaffirming his stance in an interview as late as 29 May, after the CSV file code injection had taken place.[51] The Data Protection Officer of Schleswig-Holstein initially supported Luca – also without viewing the source code – but later retracted her support in favor of decentralized models.[52] This unclear stance towards an evidently inadequate piece of software also applies to the DSK: While they criticized Luca's vulnerable centralized architecture in the above-mentioned statement, they failed to submit Luca to a thorough analysis of its compliance with data protection law.[53]

German data protection authorities' stance towards Luca has been criticized by many experts in data protection law as being politically motivated.[54] Malte Engeler states: "The accusation that could be levelled at the Data Protection Commissioner of Baden-Württemberg is that he acted in a politically motivated manner. Data protection authorities saw the pandemic as an opportunity to get rid of their bad reputation by not standing in the way of a supposedly innovative technical solution. They also appeared to be a bit impressed by the media fuss around data protection."

47 Netzpolitik.org, Mehr als 20 Millionen Euro für Luca.

48 The press statement is accessible here.

49 Die Zeit, Luca ist leider auch keine Lösung.

50 The in-depth statement can be accessed here.

51 Interview with the Data Protection Officer of Baden-Württemberg, given to the Rhein-Neckar-Zeitung.

52 Die Zeit, Luca ist leider auch keine Lösung.

53 The DSK's statement can be accessed here.

54 Die Zeit, Luca ist leider auch keine Lösung.

Tracing apps after the third wave – Belated consolidation

In Germany, the COVID-19 pandemic reached its most recent peak on 26 April 2021, with 169 infections per 100,000 inhabitants. [55]Right around that time, on 21 April 2021, the CWA's version 2.0.3 was released.[56] It included an alteration of a long-called-for feature: manual event registration.

Late update, slow reception

This feature, which is targeted at recognizing infection clusters forming at superspreader events, enables users to scan a QR code at restaurants or other event locations. When a user receives a positive test result for COVID-19 and decides to share it via the CWA, all users who were registered in the same location around the same time are warned immediately.[57]

This feature differs from Luca in two important ways: Contrary to Luca, the CWA's event registration feature never requires users to register with their contact details; all personal data are strictly pseudonymized. Secondly, in the CWA, warnings to exposed risk contacts are triggered directly after a positively tested user submits their test results, while for Luca, health authorities first have to trigger warnings.

It is not clear, however, whether the CWA's added event registration feature contributed anything to containment of the pandemic. That is due to three reasons:

Firstly, it stands to reason that the update simply came too late. As described above, by the time the update was finally released, infection rates were roughly at their peak. Only about a month later, by 1 June 2020, infection rates had sunk from 160 to 35 per 100,000 inhabitants. [58] The update was therefore absent when it would have been needed most. Henning Tillmann, who had proposed a similar idea as early as September 2020, says: "You would have needed the cluster recognition feature before the second pandemic wave. If it had been integrated into the CWA last fall before, then the federated states' legal bases would have been adapted to the CWA - and Luca probably would not have been needed."

Asked why the update took so long via a press request, the Federal Health Ministry responded: "The possibility of integration cluster detection into the CWA was already being

55 https://de.statista.com/statistik/daten/studie/1192085/umfrage/coronainfektionen-covid-19-in-den-letzten-sieben-tagen-in-deutschland/.

56 https://github.com/corona-warn-app/cwa-app-ios/releases/tag/v2.0.3.

57 Tagesschau, Im Restaurant einchecken per QR-Code.

58 https://de.statista.com/statistik/daten/studie/1192085/umfrage/coronainfektionen-covid-19-in-den-letzten-sieben-tagen-in-deutschland/.

pursued by the federal government in the fall of 2020. However, a number of fundamental questions first had to be answered in the context of technical implementation, such as implementation in the data-saving architecture of the CWA, the risk of significantly increased false-positive reports, data protection, and the Google/Apple API, which did not yet make it possible to record corresponding clusters at the time."[59]

Mr. Tillmann does not buy this excuse: "There were no difficult technical aspects which still had to be figured out. These updates were not rocket science. They could have been implemented quickly." According to Mr. Tillmann, the update came so late due to systematic shortcomings in the government's distribution of responsibilities. While he supports the CWA's general approach, he criticizes how it was handled after its release: "The Federal Ministry of Health and the RKI were simply overwhelmed with the CWA's continuous technical development. There simply was no competent body or person in charge who could have done it. The federal government should have created an advisory board and staffed it with representatives from science and civil society in order to come up with sensible updates to the CWA's core features."

Henning Tillmann elaborates that this is symptomatic for Germany's larger state of digitization: "The CWA got off to a good start, but then people just didn't think about it and that's why nothing happened for so long. The pandemic has demonstrated that digital transformation in Germany is still in its infancy."

Secondly, the update potentially could have been more user-friendly. Contrary to Mr. Tillmann's originally proposed automatic cluster recognition feature, the CWA's event registration feature requires users to actively register by scanning QR codes. Tillmann says: "What Karl Lauterbach and I proposed would have been something fundamentally different from the CWA's manual event registration feature. The CWA's big perk is that it just works in the background. What we proposed just doesn't require any proactive manual user activity, so it would have taken advantage of the CWA's biggest strength. The German government and SAP/Telekom could have proposed this feature to Apple and Google."

Thirdly, state authorities were very slow in making use of the CWA's added potential. Soon after the update's release, the Federal Commissioner for Data Protection and Freedom of Information as well as the DSK recommended to quickly adapt the federated states' legal bases so that manual contact registration for events could not only be replaced with Luca but also with the CWA. The latter's decentralized and pseudonymized event registration feature, they argued, was preferrable from the perspective of data protection law.[60] Most of the federated states, however, did not do so but kept the requirement to provide

59 The response was given in German. The translation is our own.

60 The DSK's statement can be accessed here; The BfDI's statement can be accessed here.

unpseudonymized contact data in order to enable top-down contact tracing through health authorities. At the time of writing, only Saxony has changed its Infection Protection Measures Ordinance in order to allow event check-ins through the CWA.[61] As long as other federated states do not follow suit, event hosts will still be legally required to either register their guests' personal data manually or have them use Luca.

In explaining the federated states' unwillingness to change their legal bases, Malte Engeler references the recent media onslaught on data protection law: "The framing 'data protection prevents pandemic control' had so much power that people did not dare to give up on Luca. Many responsible parties did not dare to refute this false argument. The CWA also took a lot of sustained fire and therefore some lost confidence in it. Policymakers did not realize what a treasure they had in the CWA." He elaborates that sunk cost fallacies also played a role: "The federated states had already invested several millions into Luca and it was difficult to give up on it in a way that was face-saving politically. The embarrassment of having acted too hastily and made a political mistake was simply not something to which they were willing to admit."

It thus remains to be seen whether the CWA's event registration feature will be able to unfold its full potential in a fourth wave.

Most recent added features: Digital vaccination certifications and rapid test integration

With the pandemic's third wave declining and vaccination rates rapidly rising, two new functions were recently added to the CWA:

- On 2 May 2021, with version 2.1.1 and 2.1.2, rapid test results were integrated into the CWA.[62] Initially there were some usability problems though, because not all rapid test centers were connected to the CWA. The Federal Ministry of Health now obliges rapid test centers to connect to the CWA.[63]

- On 9 June 2021, with version 2.3.2, vaccination certificates were integrated into the CWA.[64] Now, users can add their digital vaccination certificate to the CWA by scanning a QR code. These QR codes can be generated by vaccination centers or medical practices. The app then displays full vaccination coverage 14 days after the last required vaccination. Simultaneously, the RKI released the CovPass app.[65] The latter enables users to

61 MDR, Corona-Warn-App zur Kontakterfassung – Sachsen prescht vor.

62 https://github.com/corona-warn-app/cwa-app-android/releases/tag/v2.2.1; https://github.com/corona-warn-app/cwa-app-ios/releases/tag/v2.1.3.

63 Tagesschau, Vergütung für Tests soll deutlich sinken.

64 https://github.com/corona-warn-app/cwa-app-android/releases/tag/v2.3.2.

65 https://digitaler-impfnachweis-app.de/

benefit from the same vaccination certification feature without having to consent to the CWA's contact tracing – a separation which is laudable from a voluntariness and data minimization standpoint. Reports have noted that the vaccination certification feature is susceptible to fraud since QR codes can just be scanned with several devices multiple times.[66] Therefore, users will sometimes have to show a valid ID card alongside with the digital vaccination certificate.[67]

Interim conclusions

It is easy to fit the above-mentioned developments into the following narrative.

- **During the first pandemic wave,** the German government appeared to comply with most principles of responsible digital governance in an almost exemplary fashion. While at first tempted by privacy-hostile alternatives, it let itself be convinced to shift to a more privacy-friendly, decentralized approach. The CWA's release was handled responsibly: The app was developed in close cooperation with responsible data protection authorities, the source code was released to the public, demonstrating openness to feedback by independent experts. A DPIA was published, and no significant security breaches occurred. Voluntary use was mostly upheld, although choosing consent (Art. 6 § 1 letter a, Art. 9 § 2 letter a GDPR) as the CWA's legal basis was a shaky solution at best.

- **During the second pandemic wave,** the German government not only slowly lost its grip over COVID-19, but also neglected to comply with its continuous monitoring and updating obligations. While a much earlier addition of a cluster recognition feature to the CWA certainly would not have been a panacea, it would have been a valuable asset during fall and winter. It likely would have prevented numerous federated states' governments from being caught on the backfoot, thus acting hastily and without due consideration in their purchase of Luca. The failures during the second pandemic wave therefore laid the groundwork for what was to come during the third pandemic wave.

- **During the third pandemic wave,** things got out of hand – at least for a brief amount of time. As the German government quickly lost the confidence it had accrued for its management of the first pandemic wave, it found itself under pressure to look for scapegoats and simulate activity. In "data protection", a scapegoat was identified, and in Luca, a seeming quick-fix was found. This led to ill-considered Luca license purchases, questionable assessments from data protection authorities and numerous security breaches. These errors were politically hard to admit, which is why – even after it was finally

66 Der Spiegel, Warum der digitale Impfnachweis beliebig oft kopierbar ist.

67 https://www.coronawarn.app/de/blog/2021-06-10-cwa-version-2-3/

upgraded – the CWA never again really managed to play the role it could have assumed.

Malte Engeler, however challenges the narrative's delightful first part: "I used to buy into the narrative of the CWA as a success story. Now I see this more as a positive outlier which only occurred because, given Google and Apple's positioning, a centralized system would simply not have been technologically feasible." Dr. Engeler believes that, had Apple and Google not insisted on a decentralized systems, the internet community's pleas would have fallen on deaf ears: "The decentralized system was forced by Apple and Google; there is nothing to celebrate about this process."

Dr. Engeler's challenge indeed is not unplausible: What happened to contact tracing apps that did not receive Apple's and Google's approval, became readily apparent from France's *StopCovid* app. Due to its centralized design, it did not gain access to the GAEN API, rendering it effectively unusable. On 14 October 2020, French president Macron conceded that *StopCovid* "did not work"[68] and withdrew it from the market in order to replace it with a different app.

During the COVID-19 pandemic, Apple and Google advocated for a decentralized design, thus shifting public debate in a more privacy-friendly direction. The experiences with contact tracing apps' dependence on GAEN API and the shift in power that came with it, however, certainly highlight the need confront and regulate international corporations' power over digital policy. The next time we depend on their cooperation, Apple's and Google's position might not be as commendable.

68 Les Numeriques, StopCovid "n'a pas marché", place à Tous anti-Covid.

The CWA's effectiveness

Whether or not tech giants were the real force behind Germany initially introducing a privacy-friendly app, the question remains whether tracing apps actually help reduce COVID infections.

Evaluating effectiveness is not only a hallmark of good digital policy, but also a requirement of data protection law: Interferences with the right to data protection are only justified, as long as they are suitable to fulfil a public purpose. It is incumbent upon governments interfering with fundamental rights, to ascertain this suitability. If evaluations of contact tracing apps showed that they do not help reduce infections, they would have to be withdrawn and all collected data deleted as soon as possible.

Many such studies have already been conducted. A number of studies investigating Switzerland's SwissCovid app,[69] the United Kingdom's NHS COVID-19 app,[70] and Spain's radar app[71] argue that contact tracing apps work.[72]

The British study found that the fraction of individuals notified by the app who subsequently showed symptoms and tested positive was 6%, similar to manual contact tracing. Using mathematical modelling and statistical comparisons, it also found that for every percentage point increase in app uptake, the number of cases could be reduced by 0.8% (using modelling) or 2.3% (using statistical analysis). The Spanish study, conducted in the Canary Islands, found that the Spanish contact tracing app notified roughly twice the number of people exposed to simulated infections, compared with manual contact tracing. The Swiss study found that the SwissCovid app boosted the number of people in quarantine in Zurich last September by 5%, and 17% of these people tested positive. Another Swiss study found that that non-household contacts notified of exposure by the SwissCovid app entered quarantine a day earlier than did those notified through manual contact tracing.

69 There were three Swiss studies, all conducted in Zurich: von Wyl et al., Early evidence of effectiveness of digital contact tracing for SARS-CoV-2 in Switzerland, Swiss Med Wkly. 2020;150:w20457; von Wyl et al., Digital proximity tracing app notifications lead to faster quarantine in non-household contacts: results from the Zurich SARS-CoV-2 Cohort Study; von Wyl et al., The role of the SwissCovid digital proximity tracing app during the pandemic response: results for the Canton of Zurich.

70 Fraser et al., The epidemiological impact of the NHS COVID-19 app, Nature volume 594, pages408–412 (2021).

71 Rodríguez, P. et al. Nature Commun. 12, 587 (2021).

72 A short summary of these findings can be found here: Nature, Contact-tracing apps help reduce COVID infections, data suggest.

Measuring tracing apps' effectiveness: A complex undertaking

Truly understanding and contextualizing these findings, however, requires accepting one thing: Measuring "effectiveness" of contact tracing apps is a very complex undertaking. Evaluating contact tracing apps is difficult since there is no central source for data. Instead, data have to be collected from different sources – some data points simply remain unknown and have to be statistically inferred.[73]

Moreover, the term "effectiveness" can mean a lot of things. Professor Viktor von Wyl, epidemiologist at the University of Zurich, who was responsible for evaluating Switzerland's Swiss-Covid app, points to a wide array of publications discussing a research agenda for digital proximity tracing apps and the terminology of effectiveness.[74]

He elaborates: "Effectiveness occurs when more contacts are alerted more quickly than by manual contact tracing, and those contacts then end up 'doing the right thing'. In this sense, effectiveness depends on several factors, including technical ones – how well does the app measure risk exposure? - , on the users themselves – who needs the app and do users follow instructions? – as well as on the the actions of warned contacts – do they get tested or not?" Professor von Wyl goes on: "The latter also depends on societal incentives, for example whether COVID-19 tests are available for free. Effectiveness is therefore not only created by the app alone, but also by its proper embedding in the overall system."

Professor von Wyl notes that his research is limited to two sub-aspects of effectiveness: "Can more people can be warned by the app than by manual contact tracing, and does the app tend to warn risk contacts more quickly than manual contact tracing?"

He emphasizes that the larger question – whether contact tracing apps actually have a tangible effect on the pandemic – is much more difficult to measure. It is usually inferred through statistical models which each have their own blind spots and weaknesses, he says.

Professor von Wyl also points to limited resources: "I had a very small mandate from the Federal Office of Public Health, which covered only a fraction of the total costs. My work and that of my colleagues was conducted on a voluntary basis." Viktor von Wyl advocates for broader funding of such research projects in the future.

73 This difficulty is noted here.

74 Von Wyl et al., A research agenda for digital proximity tracing apps, Swiss Med Wkly. 2020;150:w20324; von Wyl et al., Towards a common performance and effectiveness terminology for digital proximity tracing applications.

Measuring the CWA's effectiveness

Since the CWA's release, the RKI has routinely released some CWA use parameters. At the time of writing, the most recent numbers were from 25 June 2021.[75] By this date, the CWA had been downloaded 29.2 million times. 29.2 million is equivalent to approximately 35.6% of the German population. 773,462 verified positive test results had been registered in the CWA, of which 475,151 (61%) had been shared. Due to the CWA's decentralized nature, certain data points, including how many users were warned through the CWA, were not included in these numbers

That is why, in March 2021, the RKI launched an effort to properly evaluate the CWA's effectiveness.[76] In so doing, the RKI mainly made use of two data sources:

- **Event-independent data donation:** In the CWA, all users were asked to voluntarily donate their usage data. These data were then evaluated through Privacy Preserving Analytics.

- **Event-Driven User Survey:** From March through May, all users receiving a status warning of "increased risk" were asked to participate in a voluntary online survey. App users were asked about their behavior before the risk notification and about their planned behavior afterwards. The second survey, which was conducted five days after the first, was designed to determine whether users who received an "increased risk" status notification actually implemented their planned behavior changes.

The evaluation's results are mostly in line with the other abovementioned studies. They point towards the CWA's effectiveness. Notably, the evaluation yielded the following results:

- On average, each user who shared their positive test results warned 6 other persons through the app.

- Approximately 73% of users receiving a status warning of "increased risk" through the app say that they were "surprised" by that warning – indicating that without using the app, they may not have registered their risk of exposure at all.

- Approximately 87% of users receiving a status warning of "increased risk" through the app subsequently get tested. Out of these users who are getting tested after receiving a risk notification through the CWA, approximately 6% are tested positive for COVID-19 –which is very similar to the equivalent rate for manual contact tracing.

According to Professor von Wyl, these results point towards the app's effectiveness in the

75 https://www.rki.de/DE/Content/InfAZ/N/Neuartiges_Coronavirus/WarnApp/Archiv_Kennzahlen/Kennzahlen_25062021.pdf?__blob=publicationFile.

76 The evaluation report can be accessed here.

above-described sense: "The methodology is convincing". He further elaborates: "The fact that many users are surprised by the warning indicates that the app registers risks outside their own household, i.e., situations where people sometimes do not know each other by name. The fact that more than 80% then got themselves tested is also a sign of effectiveness. They took the warning seriously and became active." For the near future, the RKI plans to conduct more in-depth evaluations, notably by putting their results into context with the above-mentioned international studies.

Usefulness of cluster recognition and event registration apps

Cluster recognition features have not yet been scientifically reviewed to the same extent as tracing apps' more "traditional" tracing feature. One of the most interesting questions to investigate in this regard will be whether the CWA's strictly pseudonymized and decentralized approach or Luca's centralized top-down approach help avert infections more effectively.

These two alternatives reflect an important policy choice: "The choice between centralized and decentralized event registration or cluster recognition systems depends on how much personal responsibility you trust individual citizens to bear. The central question is: Do we want health authorities in the picture or not?" Henning Tillmann emphasizes.

Understanding the two systems' effectiveness, however, is also a requirement of data protection law: Luca's centralized approach – even if it works properly and without its recent negligent security risk management – constitutes a much more serious interference with the right to protection of personal data than the CWA's decentralized and pseudonymized system. According to the principles of proportionality and data minimisation (Art. 5 § 1 letter c, Recital 170 GDPR), in order for its processing of personal information to be justified, Luca would have to be able to provide evidence, that their approach is significantly more effective than the CWA at preventing infections.

Some initial evidence suggests that Luca's centralized event registration feature may not be very effective at all. This evidence largely stems from German health authorities reporting that Luca is not very helpful for them. In a survey conducted by netzpolitik.org, only 3 out of 137 health authorities reported regularly using Luca.[77] Health authorities cite poor data quality, irrelevance of the received data, poor customer support and general work overload as reasons for not regularly making use of Luca. Many health authorities report that they usually do not work with restaurant-provided contact data lists at all.[78]

According to Mr. Tillmann, Germany's poor digital infrastructure is one of the main reasons for health authorities' limited ability to process the personal data with which Luca

77 Netzpolitik.org, Gesundheitsämter nutzen Luca kaum.

78 Die Zeit, Luca ist leider auch keine Lösung; a thorough report from the health authority of Weimar.

provides them: "German health authorities, to large extent, are still stuck in the age of fax machines. We are dealing with an administration that is working with equipment that essentially dates back to the 1980s. Health offices are not prepared for the kind of data processing that would be necessary in a pandemic."

Knowing what we know today, there currently does not appear to be a reason – neither from a policy nor a data protection law perspective – why state agencies should not adapt their legal bases to the event registration feature of the more privacy-friendly CWA. The CWA, after all, does not rely on the processing of personal data by overworked and underequipped health authorities.

Some tentative lessons

The end of the third wave does not necessarily mean the end of the story of German contact tracing apps. There still is much to learn and investigate. The Delta variant might bring about yet another surge of cases, once again challenging Germany's tech response. The above-mentioned experiences, however, do allow of the proposal of some tentative policy recommendations:

1. Data protection law poses no hindrance to innovation or public safety: Despite all ill-considered diatribes, the CWA has proven it: Data protection and data security due not stifle innovation. It is very much possible to develop data-driven solutions to public crises which both work well and respect privacy.

2. Responsible digital policy means more than making an app: Developments during the second and third wave have demonstrated that while app releases may garner the most publicity, they are by no means the only aspect of responsible digital policy. Once released, publicly deployed solutions must be continuously monitored and updated. Sound digital policy in the end comes down to the nuts and bolts of governance: Spending money intelligently on critical infrastructure. Intelligent technological solutions only work in an environment where they can flourish and fundamental rights are protected. The general congestion in so many parts of Germany's infrastructure – be it schools, public administration or health authorities – has demonstrated how underequipped Germany is in a contactless, and therefore digital environment. The pandemic has therefore once again emphasized that public money should be spent prudently and sustainably – instead of making quick, ill-considered purchases of undercooked pieces of software from some start-up in order to performatively feign the promotion of "innovation".

3. Data protection authorities must maintain their independence under political pressure: The developments around Luca have demonstrated to which extent data protection authorities can come under political pressure. It is to be expected that politicians sometimes ponder sacrificing data protection and data security in the name of political expediency. Data protection authorities, however – while their activities are always political – may never submit themselves to these incentives. They must instead perform their vital function of oversight and counterbalance, even in the face of political adversity. During the third pandemic wave, some data protection authorities failed to fulfil that role so as not to stand in the way of "innovation". This should not happen again.

4. An engaged and critical civil society is vital: The discourse around tracing apps was a prime example of the inestimable value of open social debate. Many positive developments – be it the rejection of invasive GPS data, suggestions for meaningful updates to the CWA, or the exposure of the extent of

Luca's security problems – would not have been possible without this degree of openness and commitment. We should maintain this high level of social vigilance for future digital policy debates. There is, however, some space for development. We have to get getter at conveying our message that privacy is not detrimental, but actually conducive to safety. Only when we manage to communicate this message in an understandable and persuasive manner can we ease some of the political pressure which leads policymakers to make rash decisions.

5. **Retain democratic sovereignty in the face of corporate power:** The CWA's development during the first pandemic wave can be described as an open and successful dialogue of civil society – but it can also viewed through the prism of corporate power. While this time, Google and Apple exerted their power to impose a privacy-friendly app architecture, the next time might be different. European governments should therefore seek to cooperate on an international level in order to be able to defend fundamental rights in the face of corporate pushback.

6. **Empirical research must be prepared from the start:** Tech responses to public crises can only be targeted and effective when accompanied by thorough evaluation efforts. Research can be particularly challenging when it is conducted in a privacy-friendly environment. Governments should actively incentivize and promote this research by providing the necessary funding.

The Civil Liberties Union for Europe (Liberties) is a non-governmental organisation promoting and protecting the civil liberties of everyone in the European Union. We are headquartered in Berlin and have a presence in Brussels. Liberties is built on a network of national civil liberties NGOs from across the EU. Unless otherwise indicated, the opinions expressed by Liberties do not necessarily constitute the views of our member organisations.

Website:
liberties.eu

Contact info:
info@liberties.eu

The Civil Liberties Union for Europe e. V.
Ringbahnstr. 16-20
12099 Berlin
Germany

Subscribe to our newsletter
https://www.liberties.eu/en/subscribe

Reference link to study
Please, when referring to this study, use the following web address:
https://www.liberties.eu/f/XKDH18