Trusting the Corona-Warn-App? Contemplations on trust and trustworthiness at the intersection of technology, politics and public debate

Judith Simon and Gernot Rieder
Universität Hamburg, Germany

Abstract
Ever since the outbreak of the COVID-19 pandemic, questions of whom or what to trust have become paramount. This article examines the public debates surrounding the initial development of the German Corona-Warn-App in 2020 as a case study to analyse such questions at the intersection of trust and trustworthiness in technology development, design and oversight. Providing some insights into the nature and dynamics of trust and trustworthiness, we argue that (a) trust is only desirable and justified if placed well, that is, if directed at those being trustworthy; that (b) trust and trustworthiness come in degrees and have both epistemic and moral components; and that (c) such a normatively demanding understanding of trust excludes technologies as proper objects of trust and requires that trust is directed at socio-technical assemblages consisting of both humans and artefacts. We conclude with some lessons learned from our case study, highlighting the epistemic and moral demands for trustworthy technology development as well as for public debates about such technologies, which ultimately requires attributing epistemic and moral duties to all actors involved.

Keywords
Controversy, Corona-Warn-App, COVID-19, technology development, trust, trustworthiness

Introduction
Ever since the outbreak of the COVID-19 pandemic, questions of whom or what to trust have become paramount. Should we trust individual experts, expert institutions or political actors who may or may not base their decisions on expert knowledge? Should we place our trust in individual data points, aggregated statistics or automated systems that
trace contacts and predict spread dynamics? And if we decide to rely on such tools, who should we trust to build them? This article examines the public debates surrounding the initial development of the German Corona-Warn-App in 2020 as a case study to analyse such questions at the intersection of trust and trustworthiness in technology development, design and oversight. Providing some insights into the nature and dynamics of trust and trustworthiness, we argue that (a) trust is only desirable and justified if placed well, that is, if directed at those being trustworthy; that (b) trust and trustworthiness come in degrees and have both epistemic and moral components; and that (c) such a normatively demanding understanding of trust excludes technologies as proper objects of trust and requires that trust is directed at socio-technical assemblages consisting of both humans and artefacts. Our analysis also shows that even though trust and trustworthiness are normatively tied, they can come apart: while trustworthiness invites and justifies trust, it does not necessarily evoke it. We conclude with some lessons learned from our case study, highlighting the epistemic and moral demands for trustworthy technology development as well as for public debates about such technologies, which ultimately requires attributing epistemic and moral duties to all actors involved.

**On trust and trustworthiness**

Trust is frequently evoked in public policy as a desideratum. Indeed, trust almost always appears to have a positive connotation: people mostly want to be trusted rather than distrusted, a decline in trust – be it in science, politics or the media – is usually bemoaned rather than celebrated. Trust thus appears valuable both intrinsically, that is, being valuable in itself, and instrumentally, that is, being valuable for other purposes such as cooperation, reduced transaction costs or, as in the case of the Corona-Warn-App, for encouraging widespread usage.

Trust, however, always involves risk: when we trust, we have to take a leap of faith and thus make ourselves vulnerable. Were we entirely certain, trust would not be needed. Hence, trusting always bears the risk of being let down or even betrayed by those in whom we placed trust. From a normative standpoint, trust then is not valuable per se, but only insofar as it is directed at those who are trustworthy (see Scheman, 2020). Indeed, O’Neill (2020) argues that trust is pointless and even risky if badly placed, and that the important task is to place trust well. Identifying those worthy of our trust is thus essential, yet also demanding and fallible. Two different types of errors may impact our assessments of trustworthiness. On the one hand, we may deem someone trustworthy who is not, on the other hand, we may not consider someone as trustworthy who is. If we base our trust on such faulty assessments, two types of harm can occur. On one side, we may trust someone who is not worthy of our trust, which may lead to exploitation and betrayal. In turn, not trusting someone who would have been trustworthy can also be a mistake and cause harm for both the would-be trustor and the would-be trustee. The would-be trustor misses the intrinsic and instrumental goods associated with trusting. Conversely, not being trusted or even being actively mistrusted can also be a scathing experience for the would-be trustee.

A further seemingly trivial characteristic of trust is that it describes a relation: A trusts B. However, the annotation A and B for trustor and trustee veils the fact that we use the
term trust to describe very different relations between vastly different actors. Consider differences characterizing trust relations between friends or strangers, between business partners or family members. Furthermore, while most classic accounts of trust in philosophy have been modelled on trust between individuals (see Potter, 2020), there are of course other entities that can be objects of trust, namely institutions, organizations or even generic entities such as science, the media or politics. Here again, the specificities of the trust relation matter: trust in a particular politician differs from trust in politicians or trust in politics. Trust in one’s family doctor differs from trust in medicine or the pharmaceutical industry. While we use the same terms – trust or distrust – to characterize our attitudes towards these different trustees, the specific type of relationship makes a difference to the underlying conception of trust. Moreover, and relatedly, trust hardly ever is all-encompassing, but rather restricted to specific tasks, domains or competences: A trusts B in regards to x, or A trusts B to do x, but not necessarily to do y. I may trust my mechanic to take good care of my car, but not necessarily to operate on my knee. I may trust a friend to take good care of my daughter, but not necessarily to be there in time or to cook a healthy meal. Relatedly, trust comes in degrees. There are very few people we trust absolutely, and we do not trust them in all matters.

This hints at a central characteristic of both trust and trustworthiness: they have an epistemic and a moral dimension. Trusting a mechanic to repair my car entails that he has the competence to do so, the epistemic dimension, and that he is willing to do so appropriately and without scamming me, the moral dimension. Failure in any dimension will make him untrustworthy and my trust wrongly placed, possibly leading to a feeling of anger in the former and one of betrayal in the latter case. The epistemic and moral dimensions of trust and trustworthiness have been assessed in depth in Hardwig’s (1991) seminal paper ‘The Role of Trust in Knowledge’. Analysing large-scale scientific collaborations in physics and mathematics, Hardwig argues that due to the distribution of effort and competencies,

trust is often epistemologically even more basic than empirical data or logical arguments: the data and the argument are available only through trust. If the metaphor of foundation is still useful, the trustworthiness of members of epistemic communities is the ultimate foundation for much of our knowledge. (Hardwig, 1991: 694)

This trustworthiness has both moral and epistemic dimensions. A scientist’s truthfulness, Hardwig asserts, is part of her moral character, whereas her epistemic character requires not only competence, but also conscientious work as well as adequate epistemic self-assessment, that is, the ability to know and signal also the limits of one’s competences.

Finally, one of the most controversial topics is whether or not technologies, including intangible computational processes, can also be objects of trust. Some have argued that one cannot trust technology, but merely rely on it (see Nissenbaum, 2001), which links to a central debate in philosophy concerning the difference between proper trust and mere reliance (see Baier, 1986; Goldberg, 2020). In contrast, others have argued that one may indeed use the notion of trust to describe attitudes towards technologies if they are not conceived as technological artefacts, but rather as socio-technical assemblages consisting of humans and artefacts interwoven in increasingly dynamic and complex ways
Simon and Gernot

(see Weckert and Soltanzadeh, 2020). Yet, even in those accounts, the authors seem to agree that while such relations may be more than mere reliance, there are still differences between trust in technologies and trust in other human beings. Thus, trust in a thicker sense can only be an attitude towards humans – either directly or indirectly through their involvement in institutions or their participation in technological development. Accordingly, and as the case of the German Corona-Warn-App outlined below illustrates, trust in a specific technology must not be understood as trust in the artefact as such, but rather as trust in the process of its creation and the epistemic and moral trustworthiness of the various stakeholders involved.

**Negotiating trust: The case of the German Corona-Warn-App**

On 16 June 2020, after months of controversial debate, the German Corona-Warn-App became available in the app stores of the two major mobile platforms. Through Apple’s App Store and Google Play, smartphone users could download the software that had been commissioned by the federal government in hopes of curbing the spread of the COVID-19 virus. Within the first 2 weeks after its release, the app was downloaded over 14 million times, a number that would rise to 24.2 million by mid-December 2020 (see Robert Koch Institute (RKI), 2020). In a video podcast published just days after the app’s launch, the German chancellor Angela Merkel praised it as an important tool in the fight against the pandemic that ‘deserves your trust’ (Press and Information Office of the Federal Government, 2020; transl. by authors). This call to trust, however, did not simply appeal to people’s good faith, but was accompanied by details about (a) the values that had guided the app’s development, such as transparency, privacy and security, and (b) some of the technical specificities that had been embedded in the app’s design, including decentralized data storage, pseudonymization and the decision not to collect location data. In addition, the chancellor emphasized that the Federal Office for Information Security (BSI) and the Federal Commissioner for Data Protection and Freedom of Information (BfDI) had been involved in the app’s development from the very start, allowing the tool to ‘become our companion and guardian’ (Press and Information Office of the Federal Government, 2020; transl. by authors). Importantly, its use was said to be entirely voluntary, with no additional incentive structures – that is, rewards for use or penalties for non-use – attached. The presentation and framing of the app in such a way is, of course, indicative of the difficult task to build confidence in a tracing technology in a country and culture where the protection of privacy has been a paramount concern, both as a result of a long-standing legal tradition where the right to privacy is seen as one aspect of the protection of personal dignity (see, for example, Whitman, 2004) and for more recent historical reasons, that is, the unprecedented state surveillance and intrusion on private life under authoritarian rule (see, e.g. Bloch-Wheba, 2015). In this section, we seek to provide a brief overview of the discursive arena – comprising different sites of contestation and controversy (see Clarke, 2005) – that has not only shaped the Corona-Warn-App’s technical design, but also the specific actor-network configurations in place. More specifically, we are interested in the debates and negotiations that have
accompanied the government’s efforts to build an app and support the fight against COVID via technical means.

**Phase 1 – From mobile phone location tracking to Bluetooth-based contact tracing**

In early 2020, when COVID-19 infections accelerated across the globe and the World Health Organization (2020) officially classified the outbreak as a pandemic, German research institutes and government agencies started to investigate the possibility of using mobile phone location data for contact tracking. In the beginning of March, the President of the RKI, Lothar Wieler, declared that reading movement data from mobile phones could prove to be a good way of finding people who had been in contact with infected individuals, emphasizing that the technical viability of the approach had already been established (see Schröder et al., 2020). The RKI’s proposal triggered mixed reactions. While some politicians believed that in order to deal with the public health crisis, all digital options had to be considered, others warned that there were good reasons why access to telecommunications data was tightly regulated by law, and that cell site analysis in urban areas could mean that personal data of hundreds of thousands of people would be processed without their consent. Reactions among the German Data Protection Commissioners varied as well, with some stressing the possible benefits and others noting the potential risks of the approach. Nevertheless, there was agreement that under current law, the data would either have to be anonymized or people would have to be properly informed and give their explicit consent to being tracked (see Neuerer, 2020; Schulzki-Haddouti, 2020). In addition to privacy and legal concerns, there were also doubts about the proposal’s technical feasibility. The telecommunications company Deutsche Telekom, for instance, called the plans ‘nonsense’, arguing that besides regulatory restrictions the envisaged method would not provide a complete enough picture of the situation (see Greis, 2020). The Federal Commissioner for Data Protection and Freedom of Information, Ulrich Kelber, argued along similar lines, calling into question whether the added value of relatively imprecise cell site data could indeed justify the massive infringement of fundamental rights that would follow from such an approach (see Schulzki-Haddouti, 2020). Yet, despite the scepticism on several fronts, the project continued.

On 17 March, RKI President Wieler stated at a press conference that a team of 25 people from 12 different institutions were working on a solution and that he was very optimistic that a convincing concept would soon be available (see Phoenix, 2020). What happened next, however, changed the dynamic of the debate. On 21 March, a draft bill surfaced indicating that the federal government, specifically the Federal Ministry of Health, intended to allow public authorities to request data records from telecommunication operators during national epidemics, including any data necessary to track infected persons and identify people who had come in contact with them (see Laaff and Hegemann, 2020). When the plans became public, there was immediate pushback from data privacy experts and civil rights activists, who raised doubts about the constitutional legitimacy of such a law, from academics and researchers, who emphasized that the intended methods
were not precise enough and would thus constitute a disproportionate breach of fundamental freedoms, but also from politicians of both opposition and ruling parties. In light of such strong criticism and a clear ‘no’ from the Minister of Justice and Consumer Protection Christine Lambrecht (see Tagesschau Editorial Staff, 2020), the Federal Minister of Health, Jens Spahn, had to backtrack and the passage that would have provided legal grounds for mobile phone tracking was cut from the bill. While the idea of monitoring people’s location data was not entirely dead – with Minister Spahn stressing at a press conference that ‘the topic continues to be a topic’ (Federal Ministry of Health, 2020; transl. by authors) – a different technical approach to identifying contacts started to gain ground. From April onwards, Bluetooth-based distance tracing apps were discussed as an alternative that would not grant too much power to the state but could still aid in containing the spread of the disease. Chancellor Merkel expressed her support for such a solution early on, stating that if tests would show that these apps can help with contact tracing efforts, she would ‘absolutely be in favor of recommending [the app] to citizens and of course be ready to use it [herself] and maybe help other people by doing so’ (Beuth, 2020; transl. by authors). The Chancellor, however, would have to exercise patience as various aspects of the app’s development and implementation proved to be highly controversial.

**Phase 2 – Centralized or decentralized?**

In the beginning of April, it still seemed likely that German tracing apps would be built on top of the Pan-European Privacy-Preserving Proximity Tracing (PEPP-PT) protocol, which had been developed by an international consortium of research institutions and business stakeholders from eight different countries. In essence, the protocol uses Bluetooth handshakes to register proximity events between nearby devices, thereby exchanging temporary IDs issued by a central server. In case of a positive COVID test result, users are asked to upload their contact logs to the server, which, after a series of additional privacy, security and accuracy measures,² will issue a warning to users who have been in contact with the infected individual. In the project manifesto, the consortium promised ‘well-tested proximity technologies; secure data anonymization; [and] trustworthy mechanisms to enable contact between user and health-officials in a data protection conforming environment’ (PEPP-PT, 2020a). At first, Germany’s political leadership supported the initiative. A resolution from 15 April reads:

> The federal government and the regional states hereby support the architecture ‘Pan-European Privacy-Preserving Proximity Tracing’ because it pursues a Europe-wide approach, complies with European and German data protection rules, and only stores epidemiologically relevant contacts of the last three weeks on a user’s mobile phone without recording their movement profile. In addition, use of the app should be voluntary. (Federal Government, 2020, p. 3; transl. by authors)

Despite the commitment to voluntariness, however, the resolution emphasized that it would be necessary that large parts of the population will use the app and that the government and the states will encourage this. In addition, it called upon developers of
alternative tracing apps to utilize the platform so that all offers would be compatible (see Federal Government, 2020: 3–4). Given this level of support, it already seemed certain that the PEPP-PT protocol would become the technical backbone of Germany’s digital tracing efforts. But matters turned out differently.

On 19 April, shortly after it became public that there were disagreements among members of the PEPP-PT consortium and that some members had already left the project for a lack of transparency regarding the technical nature of the project (see Sperlich, 2020), a group of 300 scientists and researchers from around the globe – 56 from Germany – issued a joint statement in which they cautioned against the use of centralized systems (see Acquisti et al., 2020). The group noted that the European Parliament (2020), in a resolution on 17 April, had recommended that in the context of contact tracing applications, ‘data are not to be stored in centralized databases, which are prone to potential risk of abuse and loss of trust and may endanger uptake throughout the Union’ (p. 11). Thus, rather than opting for solutions where ‘bad actors’ could access the social graph and spy on citizens real-world activities, they urged governments to rely on systems that are privacy preserving by design, pointing to a number of decentralized methods (e.g. DP-3T, TCN or PACT) that would ensure that citizens’ data protection rights are upheld.

A few days later, on 24 April, a coalition of six influential German organizations – the Chaos Computer Club, the digital policy-focused associations D64 and LOAD, the Forum of Computer Scientists and ITProfessionals for Peace and Social Responsibility, the German Informatics Society and the Foundation for Data Protection – wrote an open letter to Minister Spahn in which they criticized the German government’s decision to support the PEPP-PT protocol. They stressed that any tracing app should, if built at all, be based on a decentralized architecture as the insufficient privacy safeguards of the centralized approach would erode people’s trust in using such an app and undermine the acceptance of future digital solutions. The letter ended with a plea to take the objections and demands of the IT research community seriously and warned the Minister that the currently preferred solution would lead to a ‘crash landing – and that is something that nobody can afford when fighting a pandemic’ (Gesellschaft für Informatik et al., 2020).

It is not entirely clear what finally tipped the balance. Was it the conflict within the PEPP-PT consortium? Was it the critique of researchers and digital advocacy groups? Or was it the fact that the tech giant Apple had refused, despite considerable political pressure (see Krempl, 2020), to make changes to its mobile operating system to accommodate the centralized PEPP-PT approach (see Busvine and Rinke, 2020)? What is clear, however, is that the German government shifted its course radically, with Helge Braun, Head of the Chancellery, confirming on 26 April that one would now ‘promote a decentralized approach which stores contacts only on the devices themselves and creates trust’ (Becker and Feld, 2020; transl. by authors). But while the government’s decision was welcomed by critics of the centralized approach, there were still more issues that needed to be addressed.

**Phase 3: Open source, security and voluntariness**

After the government changed course, preparations for a fresh start were made. On 28 April, officials announced that the companies Deutsche Telekom and SAP had been
tasked with developing the app and bringing it to market. Corporate spokespersons confirmed that the two companies will form a team and work full speed on an open-source solution (see Neuerer et al., 2020). The disclosure of the source code had been a key request of researchers, IT experts, NGOs and opposition parties (see Böhm, 2020), and its eventual release on GitHub – with the initial concept documentation being shared on 13 May and the complete source code on 31 May – contributed to the predominantly positive reception of the app. As the German software developer and co-chair of the digital policy organization D64, Henning Tillmann, stated after inspecting the GitHub repository: ‘The source code unveiled no surprises’, which, of course, is the desired outcome if one searches for trackers and worries about data protection (Welchering, 2020; transl. by authors). Public interest in the app’s concept and code was high, with 65,000 unique visitors, 260 reported issues (i.e. tracking of problems and bugs) and 285 pull requests (i.e. suggesting modifications to the code) in less than 2 weeks after the first repositories had been posted (see Mueller, 2020). Even representatives of the Chaos Computer Club (CCC), an influential civil society organization in Germany that deals with security and privacy aspects of technology and is known for its hacker culture and rigorous software analysis, called the development process ‘exemplary’, at least in the final stages. As CCC spokesperson Linus Neumann put it: ‘The app is the first big, publicly financed open-source project in Germany. The federal government can pat itself on its back’ (Rzepka, 2020; transl. by authors).

It should be mentioned, though, that the commitment to technical transparency and external review had its limits. Experts of TÜV Informationstechnik (TÜViT), a well-respected technical service provider specialized in IT security that had been commissioned to examine the app, noted, for instance, that they were only given 2 weeks for their assessments rather than the 4 weeks the company had initially requested (see Scherschel, 2020). During these tests, the TÜViT experts had found a number of security issues which they had reported to the developers. The app’s pending launch date on 16 June, however, made it doubtful whether there would be enough time to implement the necessary changes. In addition, certain parts of the system – that is, the server backend and the frameworks developed by Google and Apple – were not included in the requested tests. Thus, while the BSI’s decision to involve TÜViT can be seen as an attempt to improve the security and transparency of the app – a collaboration the agency had declined when developing the PEPP-PT platform (Scherschel, 2020) – time constraints and the limited test scope had left a bitter aftertaste. As TÜViT Managing Director Dirk Kretzschmar summarized his verdict of the app, ‘there is some catching up to do’ (Scherschel, 2020; transl. by authors).

A final issue concerned the question of voluntariness. Just before the release of the Corona-Warn-App on 16 June, the Minister of Justice, Christine Lambrecht, clarified that the use of the app would be voluntary and that there would neither be any rewards for those who decided to activate the app, nor any disadvantages for those who decided not to (see Spreter, 2020). The Minister’s announcement followed shortly after Klaus Müller, the Managing Director of the Federation of German Consumer Organisations (VZBV), had insisted that employers, restaurants or state agencies should not be allowed to make usage of the app a prerequisite for access or service, which would undermine the principle of voluntariness and enforce the app’s use (Spreter, 2020). The three main
opposition parties had raised similar concerns, demanding a new law that would regulate how the app can be employed. Minister Lambrecht, however, rejected such demands, arguing that the rules of the European General Data Protection Regulation (GDPR) would apply to the app, meaning that ‘all questions regarding data protection [were] covered and that there [was] no need for a special law’ (Schwedt, 2020). The government, she emphasized, had opted for ‘full transparency’ with regard to the development of the Corona-Warn-App and was now hoping that many people would decide to use it.

Discussion

Having portrayed the debates around the development of the Corona-Warn-App in some depth, let us now return to the question as to whether the app is indeed a technology that one can and should trust. In order to answer this question, we will draw upon the characteristics of trust and trustworthiness outlined above, namely that (a) trust is not valuable per se, but only insofar as it is targeted at agents and activities that are genuinely trustworthy; that (b) trust and trustworthiness come in degrees and have both a moral component (i.e. being truthful and trust-responsive) and an epistemic component (i.e. being competent as well as knowing and signalling the limits of one’s own competence); and that (c) trust cannot be directed at technological artefacts as such, but only at the actor–network behind such technologies.

Let us start our analysis with aspects that have contributed to the Corona-Warn-App’s trustworthiness. When the German chancellor stated that the app deserves our trust, she did not suggest that we should blindly trust the app. Rather, she made a claim that this app is trustworthy because of the specific values that had guided its development (i.e. transparency, privacy and security), the trustworthiness of the different stakeholders, experts and institutions involved (such as the BSI and BfDI) and the concrete technological implementations chosen (a voluntary, Bluetooth-based tracing system with a decentralized data architecture), all of which was aimed at establishing credibility and justifying trust. Importantly, however, this trustworthiness did not exist from the start.

In the first phase of the development, when the focus was still on using location data for contact tracking, debates ensued questioning the trustworthiness of the project on both epistemic and ethical grounds. Epistemically, the technical feasibility of the approach was questioned, challenging the assumption that location data could be used to effectively track the disease. From an ethical – but also legal – perspective, it was questioned whether the infringement of civil liberties through invasive tracking was justifiable given the circumstances. These two perspectives were often interwoven, as shown by the response of the Federal Data Protection Commissioner, who raised doubts as to whether the added value of relatively imprecise cell site data (epistemic assessment) could indeed justify the massive infringement of fundamental rights that would follow from such an approach (ethical and legal assessment). When despite these concerns, the Federal Ministry of Health decided to prepare a draft bill that would have granted authorities access to telecommunications data, the plans again received immediate pushback on both epistemic (e.g. for being technically infeasible) and moral (e.g. for being a disproportionate breach of freedom) grounds, which eventually paved the way for a more privacy-preserving method based on Bluetooth handshakes.
In the second phase, trust and (proclaimed) trustworthiness – but also distrust – played a crucial yet contested role. While the trustworthiness of the app had already been promoted in the PEPP-PT project manifesto, it became apparent that some of the consortium members had doubts about this claim. More precisely, the lack of transparency regarding technical details of the project and open critique of its centralized architecture caused a massive pushback from experts within and beyond the consortium. It was argued that the centralized approach could open doors not only for abuse by malign actors, but also for ‘function creep’, that is, the use of a technology for purposes other than originally intended, resulting in a loss of public trust that may limit the acceptance and uptake of a voluntary system. Hence, the critics’ request for a decentralized system can be conceived as a positive form of distrust in powerful players that ultimately aimed at preventing future misuse through a solution that would prohibit such misuse by design.

With respect to Phase 2, there are a few more observations to be made. First, while it cannot be proven that the joint statement of the Chaos Computer Club, D64, LOAD, FIfF, the German Informatics Society and the Foundation for Data Protection was responsible for the government’s eventual change in course, it appears at least plausible that it had some effect. The joint statement is of interest in particular because the actors involved have a reputation of not only being epistemically trustworthy, that is, competent in digital matters, but can also be considered morally trustworthy because they are either individually politically independent – as in the case of the German Informatics Society – or collectively trustworthy due to being located at very different points of the political spectrum, ranging from LOAD, which has ties to the liberal party FDP, to D64, which is linked to the social democratic party SPD. Second, while it is important to acknowledge the role of expert advice for the government’s turn towards decentralization, one must also stress the power of platforms to set the parameters and limit the scope for political decision-making. Indeed, the final blow for the centralized approach appears to have been Apple’s refusal to change their operating systems to allow for such a centralized architecture. Given the company’s market share, this effectively rendered the PEPP-PT-based approach impossible. This outcome should alert us to our dependence on proprietary digital infrastructures and related questions of power, sovereignty and vulnerability. While in this case, corporate preferences led to a more privacy-friendly solution, the power of platforms to not only enforce but potentially also to hinder the realization of fundamental rights and values through design requirements should concern us deeply (see van Dijck, 2019).

Finally, in Phase 3, two Germany-based companies were tasked with developing a fully decentralized contact tracing app that uses Bluetooth, stores information on the individual phones and operates on open-source code. In this regard, two aspects seem particularly noteworthy from the perspective of trust and trustworthiness. The first concerns the high transparency of both the process and product, including an open-source approach allowing anyone with the relevant expertise to inspect and test the app’s technical foundations. This openness invited participation by a wide variety of actors who could – and actually did – test, correct and contest different aspects of the app’s design. Importantly, this transparency did not only foster trustworthiness, but also improved security since the code could be inspected for bugs and loopholes. Thus, the in depth-assessment of the app through actors with high epistemic trustworthiness such as the
Chaos Computer Club, and also through knowledgeable individuals who made suggestions for improvements, increased the app’s trustworthiness and in extension its legitimacy. The second aspect regarding the app’s trustworthiness concerns its voluntariness. As the Minister of Justice stressed, no advantages or disadvantages should be tied to the usage of the app and people should be able to determine freely whether they wanted to install it on their phones. Indeed, any such incentives would not only undermine the principle of voluntary use, but also a trust-based approach as such. Without the app being voluntary, talk of trust would cease making sense altogether since coercion pre-empts trust. Thus, the voluntariness of the app was on the one hand a prerequisite for it being trusted. On the other hand, such a voluntary approach required trust in the willingness of people to use the app in order to be effective.

Throughout this article, we have described the development of the Corona-Warn-App mainly as a success story where open critique and debate incrementally led to a more trustworthy design and implementation. However, not all of the actors involved would agree to such a positive depiction. Next to critique regarding the Bluetooth-based approach’s technical suitability, limited smartphone support, the initial lack of cross-border compatibility, usability problems and gaps in the testing and reporting infrastructure, a heated debate erupted over whether the project partners’ commitment to ensure that the app ‘processes a minimum of required personal data that is handled with maximum protection’ (Authors of the Corona-Warn-App Open-Source Project, 2020) was in fact undermining the app’s utility and efficacy. As the Minister President of Bavaria, Markus Söder, stated in December 2020, ‘the Warn-App could have a greater impact and help much more, but it basically fails due to the high hurdles of data protection’ (Norddeutscher Rundfunk, 2020; transl. by authors). Commentators have rejected this framing as ‘reckless’ and ‘perfidious’ (Hegemann, 2020), but the Minister President’s statement was reflective of wider dissatisfaction with the app’s performance. While the app had surpassed the 15% participation threshold that is often cited as the level of uptake necessary for an exposure notification system to take effect (see Hurtz, 2020), as of December 2020, only 55% of users with a positive COVID-19 test had decided to share their results via the app, a prerequisite for the app to function properly (see RKI, 2020). At the same time, various surveys had shown that a large number of Germans continued to have reservations and were unwilling to use the app, with one study indicating that the main reason for this refusal were not worries about privacy and data protection, but the sentiment that the app was practically useless, echoing Söder’s view who had previously called the app a ‘toothless tiger’ (Chip/DPA, 2020). However, these discussions about the efficacy and effectiveness of the app only gained ground after the app’s initial release in June 2020 and were fuelled by disappointments regarding the slow implementation of improvements and additional functionalities.4

Conclusion

Our analysis shows that through the transparent development process and the involvement of epistemically and morally trustworthy actors, the Corona-Warn-App became an example for trustworthy technology design that, as Chancellor Merkel put it, deserves our trust. Despite this affirmative conclusion, one must acknowledge that while
trustworthiness invites trust, it does not necessarily evoke it. Indeed, it can be argued that the continued public debate and the harsh criticism of the app by some actors may have had damaging impact on the public’s trust. Trust often serves as a background resource and only becomes visible when being questioned. While many people may not be fully aware of the data flows and privacy infringements in other apps, the fact that the privacy provisions of the Corona-Warn-App were debated so much may have had the adverse effect of raising doubts about the app, doubts that were further fuelled by a number of actors who actively sought to challenge the utility of the app. Thus, while morally and epistemically sound scrutiny contributes to trustworthiness, it can have negative implications for the perception of trustworthiness and thus on trust itself. Trust, as famously asserted by Baier (1986), ‘is a fragile plant, which may not endure inspection of its roots, even when they were, before the inspection, quite healthy’ (p. 260).

The Corona-Warn-App’s development was surely not without problems, yet the respective criticism and the critics themselves must also be assessed for their epistemic and moral trustworthiness. Thus, after distinguishing whether the respective critique was of an epistemic kind (e.g. questioning the quality of the app) or of an ethical kind (e.g. questioning the goals of the app or weighing different means and ends), we should assess the epistemic and ethical quality of the critique. This requires asking two types of questions. First, is the critique epistemically sound, that is, are the critics well-informed and do they acknowledge and signal both their competence, but also the limits of their competence? Second, is the criticism morally sound and not motivated by base motives such as click-baiting, self-staging or political campaigning? Trust and trustworthiness are thus not only desiderata in technology design and public policy, but also in the public debates that surround them, which ultimately means ascribing epistemic and moral duties to all actors involved. In such a distributed model, the governance of trust is spread across society and trust and trustworthiness are established through ongoing democratic deliberation (see also van Dijck’s introduction to this Special Issue). For this process to function properly, however, each and every one of us, be it in our roles as scientists or technology developers, policy advisors or policy makers, producers or consumers of information, has a dual duty to be trustworthy and to carefully and fairly assess the trustworthiness of others on both epistemic and moral grounds.

Funding
The author(s) received no financial support for the research, authorship and/or publication of this article.

Notes
1. This applies even in cases of self-trust where oneself is considered worthy or unworthy of trust (see Foley, 2020).
2. For a detailed documentation of the technical processes involved, see the project’s GitHub page at Pan-European Privacy-Preserving Proximity Tracing (PEPP-PT, 2020).
3. Initially, the PEPP-PT protocol had been conceptualized as an open platform that would support different ideas and architectures, including both centralized and decentralized approaches. In mid-April, however, reports indicated that the leaders of the consortium had
come to favour a centralized approach, causing supporters of the decentralized approach to withdraw their support and leave the project (Dachwitz and Köver, 2020).

4. As mentioned in the introduction, our analysis concludes with the initial release of the app. Further research is needed to assess both the app’s uptake and the accompanying controversies as well as the interactions between discourse and usage.

References

Acquisti A, Amann J, Bates A, et al. (2020) Joint statement on contact tracing: Date 19th April 2020 (Open Letter). Available at: https://drive.google.com/file/d/1OQg2dxPu-x-RZZETIpV-31Fa259NrpkJ/view.

Authors of the Corona-Warn-App Open-Source Project (2020) Corona-Warn-App open-source project: Data privacy and security. Available at: https://www.coronawarn.app/en/#privacy.

Baier A (1986) Trust and antitrust. Ethics 96(2): 231–260.

Becker K and Feld C (2020) Corona-tracing: Bundesregierung denkt bei App um. Tagesschau, 26 April. Available at: https://www.tagesschau.de/inland/coronavirus-app-107.html.

Beuth P (2020) Auch Angela Merkel würde eine Corona-Warn-App nutzen. Spiegel Zeitwelt. 2 April. Available at: https://www.spiegel.de/zeitwelt/apps/pepp-pt-auch-angela-merkel-wuerde-eine-corona-warn-app-nutzen-a-0866ceef-c264-4fe0-abc1-c759de85e73c.

Bloch-Wheba H (2015) Confronting totalitarianism at home: The roots of European privacy protections. Brooklyn Journal of International Law 40(3): 749–790.

Böhm M (2020) Beschluss von Bund und Ländern Experten sollen Code der Corona-Warn-App überprüfen können. Spiegel Netzzeitwelt, 6 May. Available at: https://www.spiegel.de/netzzeitwelt/apps/corona-warn-app-experten-sollen-code-der-app-ueberpruefen-koennen-a-8368af1d-466e-4c81-9d86-3f6188382fd4.

Busvine D and Rinke A (2020) Germany flips to Apple-Google approach on smartphone contact tracing. Reuters, 26 April. Available at: https://www.reuters.com/article/us-health-coronavirus-europe-tech/germany-flips-on-smartphone-contact-tracing-backs-apple-and-google-idUSKCN22807J.

Chip/DPA (2020) Corona-Warn-App ein ‘Zahnloser Tiger’? Viele halten die App für nutzlos. Chip.de, 30 December. Available at: https://www.chip.de/news/Corona-Warn-App-ein-Zahnloser-Tiger-Viele-halten-die-App-fuer-nutzlos_183211597.html.

Clarke A (2005) Situational Analysis: Grounded Theory after the Postmodern Turn. Thousand Oaks, CA: SAGE.

Dachwitz I and Köver C (2020) Covid-19-KontakterfassungRichtungstreit unter den Entwickler: innen der Corona-Tracing-Technologie. Netzpolitik.org, 17 April. Available at: https://netzpolitik.org/2020/richtungstreit-unter-den-entwicklerinnen-der-corona-tracing-technologie/.

European Parliament (2020) European Parliament resolution of 17 April 2020 on EU coordinated action to combat the COVID-19 pandemic and its consequences (2020/2616(RSP)). Available at: https://www.europarl.europa.eu/doceo/document/TA-9-2020-0054_EN.pdf.

Federal Government (2020) Telefonschaltkonferenz der Bundeskanzlerin mit den Regierungschefinnen und Regierungschefs der Länder am 15 April 2020. Available at: https://www.bundesregierung.de/resource/blob/973812/1744226/be47533c999dc84219ed8772e803d4/2020-04-15-beschluss-bund-laender-data.pdf?download=1.

Federal Ministry of Health (2020) Coronavirus: Live-Pressekonferenz mit Jens Spahn ab 13:30 Uhr (Video File), 23 March. Available at: https://youtu.be/KZwksnknXI8.

Foley R (2020) Self-trust. In: Simon J (ed.) The Routledge Handbook of Trust and Philosophy. New York: Routledge, pp. 231–242.
Goldberg SC (2020) Trust and reliance. In: Simon J (ed.) The Routledge Handbook of Trust and Philosophy. New York: Routledge, pp. 97–108.

Gesellschaft für Informatik, D64 - Zentrum für digitalen Fortschritt e.V., Chaos Computer Club e.V. (CCC), LOAD e.V. - Verein für liberale Netzpolitik, Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V., Stiftung Datenschutz (2020) Offener Brief: Geplante Corona-App ist höchst problematisch. Available at: https://gi.de/meldung/offener-brief-geplante-corona-app-ist-hoehst-problematisch.

Greis F (2020) Coronavirus: Telekom hält Handytracking von Infizierten für ‘Unfug’. Golem.de, 5 March. Available at: https://www.golem.de/news/coronavirus-telekom-haelt-auswertung-von-handydaten-fuer-unfug-2003-147073.html.

Hardwig J (1991) The role of trust in knowledge. Journal of Philosophy 88(12): 693–708.

Hegemann L (2020) Corona-Warn-App: Eine App, die niemand nutzt, nutzt niemandem. Die Zeit, December 6. Available at: https://www.zeit.de/digital/datenschutz/2020-12/corona-warn-app-datenschutz-effizienz-kontaktverfolgung.

Hurtz S (2020) Oxford-Simulation: ‘Die Corona-App fängt an zu wirken, sobald 15 Prozent mitmachen’. Frankfurter Allgemeine Zeitung, 16 June. Available at: https://www.sueddeutsche.de/digital/corona-app-oxford-studie-coronavirus-1.4937209.

Krempl S (2020) Corona-App per PEPP-PT: Kanzleramt soll bei Apple Druck machen. Heise, 23 April. Available at: https://www.heise.de/newsticker/meldung/Corona-App-per-PEPP-PT-Kanzleramt-soll-bei-Apple-Druck-machen-4708759.html.

Laaff M and Hegemann L (2020) Handytracking gegen das Coronavirus: Gravierender Eingriff, unklarer Nutzen. Die Zeit, 24 March. Available at: https://www.zeit.de/digital/datenschutz/2020-03/handytracking-coronavirus-mobilfunkdaten-standorte-virus-eindae mmung#was-laesst-sich-ueberhaupt-aus-mobilfunkdaten-ablesen.

Mueller J (2020) Corona-Warn-App: Wichtige Meilensteine in der Entwicklung abgeschlossen/Big development milestones completed [LinkedIn Blog Post], 29 May. Available at: https://www.linkedin.com/pulse/corona-warn-app-wichtige-meilensteine-der-entwicklung-juergen-mueller.

Neuerer D (2020) Coronavirus-Ausbreitung: SPD-Digitalpolitiker offen für Handy-Tracking von Corona-Patienten. Handelsblatt, 6 March. Available at: https://www.handelsblatt.com/po litik/deutschland/coronavirus-ausbreitung-spd-digitalpolitiker-offen-fuer-handy-tracking-von-corona-patienten/25616866.html?ticket=ST-7715065-W0bLdyC9csMjI4Bupa2k-ap3.

Neuerer D, Kerkmann C, Scheuer S, et al. (2020) Telekom und SAP bauen Corona-App. Handelsblatt, 28 April. Available at: https://www.handelsblatt.com/technik/it-internet/track ing-app-telekom-und-sap-bauen-corona-app/25784264.html?ticket=ST-18221928-Tt5bF myuWT3ApJtxUe9-ap5.

Nissenbaum H (2001) Securing trust online: Wisdom or Oxymoron. Boston University Law Review 81(3): 635–664.

Norddeutscher Rundfunk (2020) Die Warn-App scheitert im Grunde am Datenschutz (Video file), 19 November. Available at: https://daserste.ndr.de/annewill/Soeder-Datenschutz, videoin port33016.html.

O’Neill O (2020) Questioning trust. In: Simon J (ed.) The Routledge Handbook of Trust and Philosophy. New York: Routledge, pp. 17–27.

Pan-European Privacy-Preserving Proximity Tracing (PEPP-PT) (2020) Data protection and information security architecture: Illustrated on German implementation, 20 April. Available at: https://github.com/pepp-pt/pepp-pt-documentation/blob/master/10-data-protection/PEPP-PT-data-protection-information-security-architecture-Germany.pdf.

Phoenix (2020) Coronavirus: RKI-Pressekonferenz mit Prof. Lothar H. Wieleram ..170320 (Video file), 17 March. Available at: https://youtu.be/eKfiyuNaBew.
Potter NN (2020) Interpersonal trust. In: Simon J (ed.) *The Routledge Handbook of Trust and Philosophy*. New York: Routledge, pp. 243–255.

Press and Information Office of the Federal Government (2020) Je mehr mitmachen, desto größer der Nutzen (Audio podcast). Available at: https://www.bundesregierung.de/breg-de/themen/coronavirus/je-mehr-mitmachen-desto-grosser-der-nutzen-1762982.

Robert Koch Institut (RKI) (2020) Kennzahlen zur Corona-Warn-App, 18 December. Available at: https://www.rki.de/DE/Content/InFAZ/N/Neuartiges_Coronavirus/WarnApp/Archiv_Kennzahlen/Kennzahlen_18122020.pdf?__blob=publicationFile.

Rzepka D (2020) ‘Vorbildlich gelaufen’: Chaos Computer Club lobt deutsche Corona-App. *Zdfheute*, 16 June. Available at: https://www.zdf.de/nachrichten/politik/corona-app-launch-100.html.

Scheman N (2020) Trust and trustworthiness. In: Simon J (ed.) *The Routledge Handbook of Trust and Philosophy*. New York: Routledge, pp. 28–49.

Scherschel F (2020) TÜV-Prüfung der Corona-App: Lücken gefunden, Kritik am Veröffentlichungstermin. *Heise*. Available at: https://www.heise.de/newsticker/meldung/TUEV-Pruefung-der-Corona-App-Luecken-gefunden-Kritik-am-Veroeffentlichungstermin-4782537.html.

Schröder M, Dalg P and Voss O (2020) Mit Handydaten gegen das Coronavirus: Zugriff auf Bewegungsdaten ‘mehr als problematisch’. *Der Tagesspiegel*, 3 March. Available at: https://www.tagesspiegel.de/politik/mit-handydaten-gegen-das-coronavirus-zugriff-auf-bewe-gungsdaten-mehr-als-problematisch/25615368.html.

Schulzki-Haddouti C (2020) Datenschutz: Mit Standortdaten gegen Coronavirus ‘mehr als problematisch’. *Heise*, 6 March. Available at: https://www.heise.de/newsticker/meldung/Datenschutz-Mit-Standortdaten-gegen-Coronavirus-mehr-als-problematisch-4677679.html.

Schwedt A (2020) Corona-App: Bundesjustizministerin hält Extra-Gesetz für Corona-App für unnötig. *Zeit Online*. Available at: https://www.zeit.de/politik/deutschland/2020-06/corona-app-christine-lambrecht-pflicht-gesetz-bundesjustizministerin-datenschutz.

Sperlich T (2020) Corona-Tracing-App: Absetzbewegungen beim multinationalen Projekt PEPP-PT. *Heise*, 19 April. Available at: https://www.heise.de/newsticker/meldung/Corona-Tracing-App-Absetzbewegungen-beim-multinationalen-Projekt-PEPP-PT-4705279.html.

Spreter J (2020) Corona-Warn-App: ‘Freiwillig heißt freiwillig’. *Zeit Online*. Available at: https://www.zeit.de/politik/deutschland/2020-06/corona-warn-app-bundesregierung-keine-nachteile-nichtnutzung.

Tagesschau Editorial Staff (2020) Spahns Vorschlag vom Tisch: Lambrecht lehnt Überwachungspläne ab. *Tagesschau.de*. Available at: https://www.tagesschau.de/inland/lambrecht-bab-corona-handytat-101.html.

van Dijck J (2019) Governing digital societies: Private platforms, public values. *Computer Law & Security Review* 36: 1–4.

Weckert J and Soltanzadeh S (2020) Trust in nanotechnology. In: Simon J (ed.) *The Routledge Handbook of Trust and Philosophy*. New York: Routledge, pp. 391–404.

Welchering P (2020) Programmcode der Corona-App: Ein Quellcode ohne ‘Überraschungen’. *Zdfheute*. Available at: https://www.zdf.de/nachrichten/digitales/coronavirus-tracing-app-Quellcode-100.html.

Whitman JW (2004) The two Western cultures of privacy: Dignity versus liberty. *The Yale Law Journal* 113: 1151–1221.

World Health Organization (2020) WHO Director-General’s opening remarks at the media briefing on COVID-19: 11 March 2020. Available at: https://www.who.int/director-general/speeches/detail/who-director-general-s-opening-remarks-at-the-media-briefing-on-covid-19—11-march-2020.