University of Amsterdam

Conditions for technological solutions in a COVID-19 exit strategy, with particular focus on the legal and societal conditions

Report for ZonMw

Institute for Information Law
Faculty of Law
University of Amsterdam
Nieuwe Achtergracht 166
1018 WV Amsterdam

Amsterdam School of
Communication Research
ASCoR
Nieuwe Achtergracht 166
1018 WV Amsterdam

Dit rapport is onderdeel is van het COVID-programma van ZonMw.
Meer informatie is te vinden op www.zonmw.nl/coronaonderzoek

Conditions for technological solutions in a COVID-19 exit strategy, with particular focus on the legal and societal conditions

Report for ZonMw

Natali Helberger, Sarah Eskens, Joanna Strycharz, Gionata Bouchè,
Joris van Hoboken, Jurriaan van Mil, Jill Toh, with Naomi Appelman,
Joran van Apeldoorn, Mireille van Eechoud, Nathalie van Doorn,
Marijn Sax and Claes de Vreese

September 2021
Amsterdam

Contents

1 Introduction and summary of key findings

1.1 Introduction

Countries are no longer governed by decrees and administrative measures only. Apps, algorithms and dashboards also play a role in monitoring, informing and steering people's behaviour and, where felt necessary, enforcing government policies. One of the important lessons from the COVID-19 crisis is that digital technologies have become a central element in the government toolbox. Taking recourse to technological solutions can be advantageous in terms of speed, scalability, efficiency and cost effectiveness. However, technological solutions also come with their own 'laws', complexities, procedures, power dynamics and effects for both users and society. This crisis is not the first and will not be the last. In its recent AI Communication, the European Commission announced its intention for the public sector to become a 'trailblazer' in using AI to solve societal problems. As we continue learning from the COVID-19 debate, it has become increasingly important to consider the future role digital technology will play in society.

Contact tracing apps are one example of what we call 'technology-assisted governance solutions' (TAGs), in the sense that they are digital solutions that have been adopted by governments in response to societal problems. Relatively soon after the first lockdown, and as part of the national debate on how to re-open society, contact tracing apps became a widely discussed TAG, and a rather central one in that debate. In its Recommendation on a Common Union Toolbox for the Use of Technology and Data, the European Commission framed contact tracing apps as playing an important role in containment in the de-escalation phase and a source of information on the effectiveness of measures. The European Commission thus, spurred initiatives in member states to introduce some form of digital contact tracing technology, including in the Netherlands.[1]

The example of contact tracing apps, however, is also very instructive when it comes to some of the challenges of 'technology-assisted governance'. Shortly after the Dutch Minister of Health Hugo de Jonge first announced that the Dutch Ministry of Health was planning to use a digital contact tracing app, an intense societal debate broke out about its implications for individuals and society. Shortly after the announcement, a coalition of experts from academia, practice and civil society formulated "Veilig tegen Corona", a catalogue of ten criteria the app would minimally have to comply with. Otherwise, experts claimed, there would be no trust that the app respected fundamental rights, freedoms, security and social cohesion.[2] A few days later, a group of academics submitted a letter to the government signed by more than 200 experts warning against 'tech solutionism'. In the letter, experts pointed to the importance of extending the fundamental rights standards and rule of law requirements that apply to traditional government actions to technological solutions, as such solutions are an extension of government action. The experts also stressed the importance of considering the broader sociological context in which the digital solution is embedded and what is needed to ensure the correct functioning of that digital solution in society,

[1] European Commission, 'Commission Recommendation (EU) 2020/518 of 8 April 2020 on a Common Union Toolbox for the Use of Technology and Data to Combat and Exit from the COVID-19 Crisis, in Particular Concerning Mobile Applications and the Use of Anonymised Mobility Data', *OJ L*, vol. 114, 14 April 2020, accessed 3 June 2021, http://data.europa.eu/eli/reco/2020/518/oj/eng.

[2] Various Signatories, 'Bescherm onze gezondheid, maar bescherm ook onze rechten', Veilig Tegen Corona, accessed 3 June 2021, www.veiligtegencorona.nl.

while continuing to respect fundamental rights and freedoms.[3] Further letters and warnings followed elsewhere in Europe (and the world). The most common concerns amongst them were that technological solutions to assist governments in fulfilling their public task were more than 'just apps', that there was a great level of uncertainty about how they would affect individuals and society, and that just as with other forms of government intervention, the implementation of TAGs must live up to standards of good administration, even when it is unclear what that actually means in practice.

The implementation of contact tracing apps was unprecedented in the sense that no clear legal and ethical guidelines existed to inform the design and implementation of the app itself, as well as its broader policy implications. The intensity of the critical debate surrounding the Dutch *CoronaMelder*, as well as the sheer volume of ethical guidance documents issued in the past year, are evidence of the yet unresolved questions surrounding the use of technological solutions.[4] However, this debate has shown the **very clear societal role** research has played in clarifying conditions, identifying potential problems and shortcomings, and pointing towards solutions, more than would have happened in times of non-crisis.

This report is the result of a project funded by ZonMw, with additional funding from the SIDN fonds, entitled: '*Conditions for technological solutions in a COVID-19 exit strategy, with particular focus on legal and societal conditions'.* ZonMw special request projects are characterised by the fact that they must contribute to an ongoing societal challenge, have a short run time, and must provide insights relevant to public decision makers.

The overall research question for the project was, **"Which conditions need to be fulfilled for information technology solutions to be used in managing the exit period in the Corona crisis, with a particular focus on legal and societal conditions?"** The project's central goal and ambition was to create an assessment framework to guide policy decisions in making recommendations for the future, while also contributing to the current ongoing debate and policy initiatives, such as new legislation emerging from the COVID-19 crisis.

Before summarizing the main findings and lessons learned from this project and explaining the structure of the report, some background will be given on the general context of this research as it has important implications on its set-up and presentation.

The role of policy research in times of crisis

The Corona crisis has thrown a new light on the role research and academics play in society—both from the perspective of the public, as during the crisis, academics have been far more visible and prominent in daily public debates, as well as the active role that teams of researchers in the form of the Outbreak Management Team (OMT) have played in actual crisis management and the development of policies surrounding it. On the one hand, the pandemic clearly created an urgent need for experts to help navigate an unprecedented societal challenge, contributing to evidence- or at least expert-based policy making. On the other hand, it also contributed to the politicisation of research, placing academics in the middle of policy making and public debates and often in ways researchers were not prepared for. From the perspective of academics, including those on our team, they found themselves and their work thrust into the public spotlight, requiring them to balance their core task of doing research with competing demands for their time from policy makers, the media, social media, and critics on social media, including politically motivated individuals seeking to target their work for their own political agenda. For some

[3] Various Signatories, 'Letter to Minister-President Rutte, minister De Jonge, Minister Van Rijn, Minister Grapperhaus and Mr. Sijbesma', 13 April 2020, http://allai.nl/wp-content/uploads/2020/04/Online-versie-Brief-Minister-President-Rutte-Ministers-De-Jonge-Van-Rijn-Grapperhaus-de-heer-Sijbesma-inzake-COVID-19-tracking-en-tracing-en-gezondheidsapps.pdf.

[4] Ministerie van Algemene Zaken, 'Testbewijs en app CoronaCheck - Corona virus COVID-19', https://www.rijksoverheid.nl/onderwerpen/Corona virus-COVID-19/algemene-Coronaregels/cijfers-en-onderzoeken-over-het-Corona virus/Coronacheck.

academics, the shift in focus from research to valorisation being in the spotlight was unfamiliar territory, highlightening the importance of training future generations of researchers in publicly communicating research findings to the media or politicians.

Closely related to the societal importance of academic research are **questions of speed and the form of communication**. Academia and academic research typically have its own pace and forms of communication (e.g., via peer reviewed journals or academic reports) that often do not match, and, in the worst case, conflict with the speed of law and decision makers, especially their willingness to read lengthy reports and peer-reviewed scientific papers. In other words, some traditional forms of reporting academic work do not lend themselves well within the context of crisis.

The Corona crisis and discussion around contact tracing apps also challenges traditional forms of doing research in other ways. Due to the breadth and multidisciplinary character of the research as well as the limited time and budget available, **new forms of conducting research were needed: i.e. more multi-disciplinary team science, but also research that was more participative, geared at integrating the perspectives of societal stakeholders.**

With the growing complexity and high-speed integration of digital technology as part of the solution to societal problems, there needs to be more flexibility when considering and budgeting for new forms of team science in the widest sense. But there also needs to be greater flexibility in acknowledging contributions outside traditional peer-reviewed publications, acquired research funding, and delivered keynotes. This is particularly important for younger researchers who have not yet reached tenure.

Implications for the research in this particular project and our report

As a result of the observations above, this project differs in a number of aspects from traditional academic projects. First of all, the research was commissioned by ZonMw in response to the critical debate around the *CoronaMelder* and the need for more evidence-based guidance and insights to aid the government in adopting and adjusting its policies. Practically speaking, this meant that the project's contribution to an urgent societal debate was central, though the debate itself is a moving target. While writing this summary, several new apps—the *CoronaCheck* app and the European Green Pass[5]—and a new legislative proposal are in the making, while other legislation we discussed in our report (e.g., the draft law concerning the collection of mobile phone data) has been subject to far more intense discussions and delays than originally expected. The combination of having a broad scope, urgency, and the topic itself being moving target has had important implications not only for the content of the research, but also how it was conducted and communicated, not to mention how we saw our roles as researchers.

First, we decided to communicate our research findings not only in a report once the project was finished, but to shift our main focus to sharing our results throughout the project in regular project updates via ZonMw, blogs, media interviews, op-eds, workshops and conversations with experts and policy makers, letters to parliamentarians, one pagers for our website, contributions to conferences, expert meetings, and finally via social media (for an overview, see appendix 2). This choice also informs the shape of this final report. It consists of this introduction and an overview of the main lessons learned, a collection of expert opinions, our various contributions to the media, and a number of thematic chapters informed by our work. Many, if not most, of these chapters have been submitted to conferences and expert meetings and shared in the form of one-pagers or op-eds with decision makers and the wider public.

Second, unlike many traditional academic research projects, we saw our primary role and task as that of critical observers and watchdogs. In other words, an important portion of the work of this team (more on

[5] European Commission, 'EU Digital COVID Certificate', Text, accessed 3 June 2021, https://ec.europa.eu/info/live-work-travel-eu/Corona virus-response/safe-COVID-19-vaccines-europeans/eu-digital-COVID-certificate_en.

the team below) went into critically following how debates around contact tracing apps and the relevant legal proposals unfolded, as well as understanding and evaluating the practical impact this had on users and society.

Therefore, an important contribution of this project was setting up a workable monitoring framework. We did so: a) through composing a multi-disciplinary team whose members would follow the relevant developments from their respective perspectives, b) by discussing our findings in weekly project meetings, including asking how they informed our research, interactions with the media, public and decision makers, and our monitoring framework, which consisted c) of a representative longitudinal survey of the Dutch population on its perceptions of, experiences with, and potential disadvantages experienced by using contact tracing apps and other digital solutions.

Third, as the topic of this research required combining a broad set of disciplinary perspectives, we had to experiment with ways of including and working with them while staying within the project's allotted time and budget. Our team included not only legal scholars, but also an ethicist, sociologist, economist, computer scientist, and several communication scholars. In addition, and to ensure that we could learn from as many relevant sets of expertise as possible, we worked with the active support of an Advisory Team (see appendix 1), consisting of leading experts from diverse disciplines who are also active in the debate around contract tracing, to complement our team.[6] Finally, we commissioned three expert opinions from researchers with complementary sets of expertise to inform our research (sections 6, 7 and 8).

Fourth, the particular character of our research as a monitoring investigation, its societal role, and limited time frame and budget, also meant that in choosing what to investigate in depth, we were led by the actual debate and the kinds of research that would best inform it. For this reason, we focused on contact tracing and sharing mobile data, not only because these were the most widely discussed TAGs, but also because they were subject to the drafting of new laws.

1.2 Outline of this report

In the following section we will briefly summarise our main research findings and lessons learned for the use of TAGs when moving forward (section 1.3).

The overall goal of this project was to monitor the implementation of the CoronoaMelder and its individual and societal implications. Sections 2-8 present our background research and expert opinions that informed our work, some of which will be turned into research papers. More concretely the subsequent sections include:

- The results of a mapping exercise of COVID-19 digital applications and the main societal, ethical and legal concerns (insights that informed our legal and policy analysis, as well as our monitoring framework) (section 2)
- A legal investigation into the regulation of mobility data for public health (section 3)
- A comparative legal investigation into the regulation of contact tracing apps across Europe (section 4)
- A comparative research into the political considerations behind different regulatory approaches (section 5)

[6] The role of the Advisory Team was in particular to advice on scoping of the research and validate our mapping of digital applications and potential societal concerns as well as to provide feedback on the monitoring framework. All mistakes and ommissions are entirely those of the authors.

- Three expert opinions on:
  - The ethical issues of invasive technologies by David van den Berg, Lisa de Graaf & Mirko Tobias Schäfer
  - The Googlization of Pandemic Response: ethical concerns regarding digital contact tracing and big tech by Tamar Sharon
  - An economic evaluation of the CoronaMelder by Joost Poort (section 6, 7 and 8).
- Our monitoring framework in the form of survey questions and results of our empirical work (section 9).
- The composition of our Advisory Expert Team (appendix 1)
- A collection of our contributions in the media, the public and academic discourse (appendix 2).
- The codebook (appendix 3).

1.3 Summary of the main findings and insights learned for the future

Insight one – There are many potentially useful digital solutions to choose from

Digital technologies can be a useful solution in responding to a number of different concerns and needs, for example, when dealing with a public health crisis such as the COVID-19 crisis. Contact tracing apps are one example, but many different technological solutions exist for a range of challenges, including:

- diagnostic technologies (to efficiently detect and contain the spread of infections e.g., through identification/detection, self-reporting mechanisms and alerts),
- evidence and monitoring technologies (to continuously assess the situation through evidence and information gathering, e.g., in the form of dashboards),
- productivity tools (to ensure that society can continue to function in times of crisis, including remote working platforms and tools), as well as
- law and policy enforcement technology (to effectively uphold existing and new precautionary and contingency measures, such as keeping a 1.5-meter distance or dispersing crowds in parks.

We found that in the Netherlands (as well as in the majority of Europe), the main thrust of government-driven digital interventions concentrated relatively quickly on the widescale distribution of digital contact tracing apps and the use of mobile data. One of the criticisms expressed by experts was there was too little discussion on investing in other, potentially more effective and necessary digital solutions. Arguably, the European Unions' push for these two solutions contributed to this situation.[7] Having said this, the media and government also played a role in centring public debate around a number of specific technological solutions while others were adopted below the radar of public scrutiny (such as the repurposing of technologies used in the area of law enforcement towards COVID-19 enforcement).

Different technological solutions possess different advantages, but also concerns. Based on a systematic mapping exercise, we found that though much of the more visible policy discourse often concentrates on privacy issues, there is a much broader range of concerns to consider, including matters of security, function creep, the normalisation of new forms of surveillance, the need for transparency and adequate communication, and closely related, that of public trust (in governments and platforms); concerns also include issues of digital inequality, the privatisation of the enforcement of public health policies, and the limited ability of users to dispute this (see also sections 2 and 6).

[7] European Commission, 'Commission Recommendation (EU) 2020/518 of 8 April 2020 on a Common Union Toolbox for the Use of Technology and Data to Combat and Exit from the COVID-19 Crisis, in Particular Concerning Mobile Applications and the Use of Anonymised Mobility Data', vol. 114, para. 2.

A reoccurring concern we identified in relation to most of the technological solutions adopted in response to the crisis concerned the potential normalisation of these solutions, and their fusion into permanent infrastructures of surveillance and increased control of citizens, not to mention the future re-purposing of these technologies for other commercial or governmental ends. As such, these interventions cannot be seen as separate from the ongoing push to digitize society and reinvent all aspects of work and life in the light of new technologies such as AI, cloud computing and the Internet of Things. The COVID-19 crisis, if anything, has only accelerated this trend and many digital interventions adopted during this time are likely to set a future precedent.

Insight two – Away from tech-solutionism, and towards a broader vision on the use of TAGs

For governments to be able to make informed decisions about which technologies to invest in and use, it is first critical to be aware of the different technological choices, the kind of problems that need solving, the concerns, potential drawbacks, and added value that accompanies each kind of technology, as well as its costs—economic, as well as the costs for society and individuals. Only in this way can governments live up to their obligation to act in accordance with their citizens' fundamental rights, and therefore adopt necessary solutions that are proportionate to and provided for by the law. In addition, our research has pointed to the fact that those countries that have been relatively successful in using technology to deal with the crisis (such as South Korea, Japan and Taiwan) have done so through a combination of technological solutions and policy choices, regarding the broader conditions that need to be realised in order for that technology to work (such as the availability of testing capacity, response infrastructure, public communication strategies, etc.). Put differently, there are no easy technological fixes, and in order for a technological solution to work, it needs to be part of a broader vision on what such a solution needs to function in society, while achieving its intended goals.

In this context, one issue we identified was the lack of concrete benchmarks and parameters to assess whether the technological solution was indeed effective in achieving its goals. The lack of concrete benchmarks also made the evaluation of the CoronaMelder very difficult. We suggest this lack of clear assessment criteria is rather symptomatic of the lack of a broader government vision on TAGs. In our report, we argue that defining such assessment criteria upfront is an important element of good administration and decision making.

Insight three – The decision to implement a particular technological solution is a political decision and should be democratically legitimized

An important common feature surrounding debates about contact tracing apps and other technological solutions is that they are presented essentially as 'just another app' or as an example of how digital technologies can help solve societal problems. The notion of it being an 'app' is already misleading, as it invokes the image of a piece of software that users can voluntarily download and remove without further consequences.

Technological interventions, such as the introduction of contact tracing, proctoring, the introduction of productivity apps, and immunity passports, etc., are more than just apps or a simple decision to invest in IT.[8] As the Council of Europe already pointed out early on in the debate: "What is ahead of us belongs

[8] Misuraca & van Noordt describe this as the "eGovernment rhetoric legacy" in the sense that the provision of ICT-enabled services would mainly involve the translation of administrative procedures into digital format and that technology is still widely seen as something separate from policy making or government reform. The authors point to the far more transformational consequences of the wider proliferation of AI in public service.
European Commission. Joint Research Centre. Misuraca, G. and Van Noordt, C., AI Watch, 'Artificial Intelligence in Public Services: Overview of the Use and Impact of AI in Public Services in the EU'. (LU: Publications Office, 2020), accessed 4 June 2021, https://data.europa.eu/doi/10.2760/039619.

to *political choices*, to societal support and to our individual commitment. Despite the urgency, digital contact tracing raises new questions that cannot be neglected before deciding to implement such population wide measures. Beyond privacy and data protection considerations, digital contact tracing approaches raise questions of inequality and discrimination that also have to be considered."[9] (highlights by authors). Philip Alston, special UN rapporteur on Human Rights, warned in no uncertain terms that the push for the digitisation of governance often treads a precarious line between digital innovation and the dangers of profound human rights violations, such as creating an excuse for setting up governmental surveillance and playing into the hands of corporate interests.[10]

While the decision to implement contact tracing apps (or other technological solutions) is often framed as a simple question about software deployment, the Council of Europe's quote makes it clear that considering if, and which technology to adopt, is deeply political. It is a matter of how to govern the public and achieve the values inherent in that society; therefore, it becomes a question about democratic legitimisation and oversight, just as with the decision whether or not to adopt a law. This is also true for the design choices inherent in these apps (centralised or not, in cooperation with external parties or not, processing of personal data or not, and under whose authority). These are choices that can have a lasting effect on the distribution of responsibilities and power in a society.

Moving forward, one important lesson to draw from the COVID-19 crisis is the need to critically scrutinise if adequate public forums and procedures exist to enable and maintain democratic control over technology. Certainly, the role of Parliaments in creating the legal basis on which governments can act remains pivotal. Yet during the COVID crisis, many critical decisions were taken outside Parliament, e.g., in the negotiations between governments and tech companies, in which the Parliament was only involved at a later stage, once the technology had already been built and its parameters set. Also, we must question whether the digitisation of governance requires new forms of transparency and democratic accountability, and if so, how those processes should be designed. To return to the example of the Netherlands, in response to the Dutch government's initial plans to roll out the app, the Ministry of Health initiated the process of public scrutiny of the app itself, including an appathon and an open-source trajectory in its second development phase. At no point in time, however, did the Ministry ask whether this particular technological solution was appropriate as a potential solution. In the various expert committees that accompanied the development of the app, none offered the room to debate this question. What is more, as Cattuto and Spina argue, "[t]he institutionalisation of digital tools for COVID-19 is … taking place within a system of public governance that is unprepared to tackle the ethical, social and legal challenges of these technologies."[11] In other words, not only should we critically scrutinise the forums and procedures that exist to enable democratic participation regarding whether or not the government should employ a particular technology, we also have to create procedures and institutions to deal with the potential wider societal and ethical implications, beyond questions only relating to data protection. Moving forward, we agree with Miscuraca that ICT-enabled innovation cannot be decoupled from public administration reform.[12]

Insight four – Consent is not a proxy for democratic legitimisation

Our in-depth, comparative review of how contact tracing apps were debated and introduced in four EU member states (Germany, Italy, the UK and the Netherlands) uncovered an important pattern: in public debates and official communications, issues of fundamental rights and user rights quickly converged

[9] Council of Europe, 'Joint Statement on Digital Contact Tracing by Alessandra Pierucci, Chair of the Committee of Convention 108 and Jean-Philippe Walter, Data Protection Commissioner of the Council of Europe', 28 April 2020, https://rm.coe.int/covid19-joint-statement-28-april/16809e3fd7.

[10] OHCHR, 'World Stumbling Zombie-like into a Digital Welfare Dystopia, Warns UN Human Rights Expert', accessed 4 June 2021, https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=25156.

[11] C. Cattuto and A. Spina, 'The institutionalisation of digital public health: Lessons learned from the COVID-19 app', *European Journal of Risk Regulation*, 11:2 (2020), 228–35, https://doi.org/10.1017/err.2020.47

[12] European Commission. Joint Research Centre. et al., *AI Watch, Artificial Intelligence in Public Services*.

around matters of privacy, and more narrowly, data protection. These concerns were either addressed by assurances of anonymisation of the collected data or by the voluntary nature of informed consent. The example of Germany was instructive. In Germany, originally a law to legitimise the use of contact tracing apps was envisaged, but soon cancelled due to the voluntary nature of using contact tracing apps and free user choice (see section 4.1). In the Netherlands, the government maintained that consent would suffice as a legal basis for public intervention.[13]

Based on our research, we question the voluntary nature of consenting to a technological solution in times of crisis. Indeed, our empirical research demonstrated that peer and social pressure were the primary motivation for users to download the app (see section 9). More importantly even, individual decisions to consent to the use of a certain technologies can never be a proxy for a societal (or democratic) decision to make those technologies part of a nation-wide response to a crisis, thereby legitimating the economic and social costs that accompany it. This tendency to substitute democratic legitimisation with expressions of individual consent brings us back the warning of political philosopher Mouffe, namely that ‘this tendency to privilege exclusively the liberal component and to present the democratic element as having become obsolete has serious political consequences’,[14] including the consequences for those that either did not want to or were not able to consent. This is why we conclude that the introduction of digital technological solutions that affect fundamental rights needs to be legitimized by law, proportionate and necessary in a democratic society and for legitimate aims.

In our report, we also explain why, both from a perspective of democratic legitimacy and fundamental rights, the use of technology assisted government solutions requires a regulatory framework (see section 3.2). In other words, informed consent in the sense of data protection law can provide legitimate ground for the processing of personal data. However, individual consent does not provide legitimate ground for the introduction of systemic data-driven solutions to support government action. The legal function of consent therefore should be interpreted narrowly and in the light of the original purpose of data protection law. With the growing proliferation of data-driven solutions, there is a tendency to view the overreliance on consent as legitimate grounds for introducing digital technologies. This tendency corresponds to another tendency of reducing concerns around data-driven technologies to matters of data protection, disregarding other important legal considerations e.g., in the area of consumer protection, non-discrimination law, health law, the freedom of assembly, the freedom of movement, etc. To some extent, this tendency is understandable: with the GDPR, a comprehensive and standardised framework for dealing with personal data has been created. And yet, as our empirical investigation has also shown, many concerns around the adoption of digital solutions were not (only) about data protection but were more widely reaching (see summaries of the empirical research in section 9). If anything, this crisis has highlighted the need for more concrete legal guidance on the legal requirements TAGs need to live up to (see also insight no. 7).

Insight five – Inclusion of non-users and vulnerable communities into technology assisted policy making

A common feature in most paramount debates around the introduction of TAGs is the focus on the users of those technologies, their concerns, fundamental rights and communication needs. Relatively less attention was invested in the non-users, i.e., those that for one reason or other were either unable or unwilling

[13] ‘Tijdelijke Wet Notificatieapplicatie COVID-10: Memorie van Toelichting’, n.d., 15, https://www.eerstekamer.nl/wetsvoorstel/35538_tijdelijke_wet; European Commission, ‘Mobile Applications to Support Contact Tracing in the EU’s Fight against COVID-19 Progress Reporting June 2020’, June 2020, 9, accessed 4 June 2021, https://ec.europa.eu/health/sites/health/files/ehealth/docs/mobileapps_202006progressreport_en.pdf.

[14] Chantal Mouffe, ‘Which Public Sphere for a Democratic Society?’, *Theoria: A Journal of Social and Political Theory*, no. 99 (2002), 55–65.

to benefit from technological solutions. The ongoing discussion around immunity passports is a case in point as a technological solution with potentially significant exclusionary effects. Being able to benefit from immunity passports depends on a number of factors, some of which are simply not within an individual's control, such as the availability and affordability of tests and vaccines. Similarly, the introduction of digital content tracing apps or online proctoring solutions are focused mostly on the fundamental rights and affordances of those using the technology, but for certain groups in society these technologies were never a solution in the first place: students with unstable internet access or having no private place to sit undisturbed, elderly people without smartphones, or those that could not afford newer smartphone models, as well as those that have refused to use these technologies due to their concerns about reliability, privacy, etc. More discussions are needed about the extent to which these solutions affect the fundamental rights and interests of non-users.

From a public values perspective, digital technologies, including apps and mobile phones, can exacerbate digital exclusion and digital inequalities that shape and define people's socioeconomic opportunities, especially during (and after) a crisis.[15] In particular, given the increasing dependency on technology, digital inequalities have to be accounted for. It puts the most digitally disadvantaged at greater risk, not simply increased vulnerability to the virus (such as eHealth literacy, or access to healthcare services), but also increased vulnerability to the repercussions of the crisis (such as maintaining daily life activities, cybersecurity issues, or gathering social support).[16]

This is another important consideration as to why technological solutions must be understood within the broader socio-technological context in which they are supposed to operate, including their non-context, i.e., the effect on those for whom these solutions are either unviable, or who are structurally left out or disadvantaged by the focus on technological fixes. Good governance with regards to technological solutions therefore also requires careful consideration of those left out, excluded or vulnerable to individual and societal disadvantages, as well as the need to draft alternative, non-technological options.

Insight six – TAGs have the potential to create new, or re-enforce existing structural dependencies to (very large) technology companies

A topic that has so far received surprisingly little *regulatory* attention concerns the role of private tech companies in the deployment of digital COVID-19 solutions. With the Exposure Notification framework, Google and Apple joined forces to "help governments and health agencies reduce the spread of the virus, with user privacy and security central to the design. "[17] In using the Google-Apple Exposure Notification Framework, governments readily outsourced yet another of their public core tasks to big tech companies, thereby further deepening the dependency on what are essentially very large commercial operators. At the same time, governments and health agencies have been given no rights to transparency or control regarding the code and protocols of those platforms.[18]

While concerns about the resulting power asymmetries and lack of public control figured rather prominently in the policy debates about contract tracing solutions, these concerns only made it, in very few exceptional cases, into national regulations or policies (see sections 4 and 5). So far, only three member states, Switzerland, Belgium and Italy, have adopted formal regulations referring to the involvement of third parties, and these were limited to prohibiting third parties (like platforms) from accessing data

[15] Sofia Ranchordás and Catalina Goanta, 'The New City Regulators: Platform and Public Values in Smart and Sharing Cities', Computer law & Security Review 36 (2020) (online first)

[16] Elisabeth Beaunoyer, Sophie Dupéré, and Matthieu J. Guitton, 'COVID-19 and Digital Inequalities: Reciprocal Impacts and Mitigation Strategies', *Computers in Human Behavior* 111 (1 October 2020): 106424, https://doi.org/10.1016/j.chb.2020.106424 .{\\i{}Computers in Human Behavior}

[17] 'Privacy-Preserving Contact Tracing - Apple and Google', Apple, accessed 3 June 2021, https://www.apple.com/COVID19/contact-tracing.

[18] Michael Veale, M., 'Sovereignty, privacy and contact tracing protocols'. In L. Taylor, G. Sharma, A. Martin, & S. Jameson (Eds.), Data Justice and COVID-19: Global Perspectives (pp. 34–39). Meatspace Press, 2020.

gathered via the app, thereby largely repeating provisions already established in the GDPR. If there were agreements made between national governments, Google and Apple on the contact tracing framework, they are, to the knowledge of the authors, unavailable to the public.

By outsourcing vital parts of public health policy to private corporations, national governments are not only creating new functional dependencies (use of the operating system), but also institutional dependencies and institutional power[19] that ultimately have the potential to affect the political landscape for decades to come (see also section 7). As Busemeyer and Thelen observe, the delegation of public tasks to private players will set in motion irreversible dynamics of dependency ("strong feedback effects") while the effectiveness of the threat of regulation will diminish over time.[20] It is important to realise that digital solutions mostly rely on broader (and less visible) computational infrastructures to capture users' physical interactions and their data, while agreeing to protect their privacy. In this sense, contact tracing apps and other digital technologies, align with Big Tech's extractivist moves to take hold of public infrastructure.[21]

It is critical to be aware of the process by which public infrastructure becomes tech infrastructure, in which technology companies underpin public infrastructure without public debate, including the partnerships and deals being pursued. As our public sector becomes more dependent on computational and technology infrastructures, it becomes increasingly important to address these dependencies and the shift in the delegation and sharing of public responsibilities with private actors. Initiatives such as the Amsterdam Procurement Guidelines are important first steps in that direction.[22]

Insight seven – TAGs require novel forms of organising democratic accountability and continuous monitoring

We have also seen that due to the particular complexity of technological solutions, traditional forms of decision making are limited and new ways of including experts and the public are needed for healthy debate. This should include a debate of which groups in the public to actually include and how to do so meaningfully, taking into account those in society that are often excluded or have no access to the policy making process. In the Netherlands, we have seen interesting approaches to organising transparency (e.g., in the form of an appathon)[23] as well as the structural inclusion of experts at all stages of decision making. Even if in practice, there is ample room for improvement moving forward, for example in terms of inclusion of also vulnerable groups and more diverse disciplinary perspectives and public accountability of government decision making.

We have seen, for example, that most of the discussion of government efforts and the public scrutiny of TAGs has typically concentrated on the introductory phase. As mentioned elsewhere, not only do these technological solutions have the potential to become permanent or re-purposed, but they are also often not in their final version when implemented and rolled out on a larger scale. Constant beta-testing, further development, and patching are all important elements of agile technology developments. As individual and societal implications are often difficult to predict, it becomes clear that constant monitoring and re-evaluation are important elements of organising democratic accountability and better policy making. Technological development has moved towards more agile forms of development, potentially leading to tensions between the pace of development and the legislative processes that govern them.

[19] Marius Busemeyer & Kathleen Thelen, World Politics , Volume 72 , Issue 3 , July 2020 , 448 - 480.

[20] Ibid.

[21] Miriyam Aouragh et al., 'The Extractive Infrastructures of Contact Tracing Apps', *Journal of Environmental Media* 1, no. 2 (1 August 2020): 9.1-9.9, accessed 4 June 2021, https://doi.org/10.1386/jem_00030_1.

[22] 'Public Procurement Conditions for Trustworthy AI and Algorithmic Systems', *NGI* (blog), 21 April 2021, accessed 4 June 2021, https://research.ngi.eu/public-procurement-conditions-for-trustworthy-ai-and-algorithmic-systems/.

[23] For a description of the process see https://www.rijksoverheid.nl/actueel/nieuws/2020/04/17/zeven-apps-doen-mee-aan-publieke-test-komend-weekend, accessed 4 June 2021

As the European Commission states in its Better Law-Making Guidelines, "One of the key qualities of good policy development is that implementation is subject to review and reflection, so that lessons are learned, adaptations are made, or even policy is abandoned in response to findings."[24] In its AI 2021 Communication, the European Commission clearly indicated the need for, and announced further actions regarding the establishment of "metrics and methods to assess and monitor the impact of AI systems on environmental and societal well-being, inclusion and diversity, as well as measures to ensure trustworthy AI in public procurement."[25]

While established procedures, responsibilities and methodologies exist for traditional acts of policy making, this is far less so for technology assisted government solutions. Returning to the contact tracing example, one conclusion from our research concerns the lack of clear key performance indicators that would have measured the efficiency of the Dutch CoronaMelder. Part of such a measurement should be cost efficiency (see section 8), but also efficiency in terms of reaching the measure's intended goals (see section 6 on an ethical assessment framework). For example, a stated goal of the CoronaMelder was to aid the Dutch exit-strategy. Ongoing assessments of the CoronaMelder focused primarily on whether or not it successfully complemented the contact tracing strategy.[26]Also, most evaluations concentrated on the functioning and general adoption of the app itself, not its broader societal implications (e.g., the question of whether the app succeeded in opening up segments of social life, and whether it affected certain individual members of society disproportionately). Monitoring the broader societal impact was a task for our research project, but this was an incidental project with limited run time. Moreover, the lack of concrete KPIs made such monitoring difficult. To the degree that governments are moving towards greater use of digital solutions, systemic and systematic solutions to monitor those effects after adoption are also needed. When doing so, it is important to be aware that questions of efficiency are always political and as such, it is significant to consider who will be involved in the monitoring process. The harm inherent in the use of certain technologies impacts the most vulnerable, who are the least represented in any form of (political) discourse.

Finally, we conclude that monitoring the success of a technological intervention should never be limited to the technology itself, but also include the success of the accompanying policy. In the Netherlands, for example, the success of the *CoronaMelder* in its initial months was limited by the fact that a warning would not in itself be a sufficient reason to request a COVID-19 test.

Insight eight – Minimum requirements for a legal framework

Based on a comparative overview of the regulatory framework in those countries that decided to regulate contact tracing apps, we identified five key issues that require additional regulation (and are not addressed by the GDPR) (see sections 3 and 4):

voluntariness,

The act of not downloading a contact tracing app should not entail any disadvantages, except for the lack of an exposure notification.

[24] European Commission, 'Commission Recommendation (EU) 2020/518 of 8 April 2020 on a Common Union Toolbox for the Use of Technology and Data to Combat and Exit from the COVID-19 Crisis, in Particular Concerning Mobile Applications and the Use of Anonymised Mobility Data', 114:88.

[25] https://digital-strategy.ec.europa.eu/en/library/communication-fostering-european-approach-artificial-intelligence, p. 33, accessed 4 June 2021

[26] Ministerie van Volksgezondheid Welzijn en Sport et al., 'Eindrapportage CoronaMelder Evaluatie', rapport, 17 February 2021, https://www.rijksoverheid.nl/documenten/rapporten/2021/02/24/eindrapportage-Coronamelder-evaluatie-tilburg-university-17-februari-2021; Ministerie van Algemene Zaken, 'Resultaten CoronaMelder', 14 October 2020, https://www.rijksoverheid.nl/onderwerpen/Corona virus-app/resultaten-praktijktest-en-uitvoeringstoets-Coronamelder; Ministerie van Volksgezondheid Welzijn en Sport, 'Evaluatie CoronaMelder - Een overzicht na 9 maanden - Publicatie - Rijksoverheid.nl', 29 May 2021, https://www.rijksoverheid.nl/documenten/publicaties/2021/05/28/rapporten-evaluatie-Coronamelder-9-maanden, all accessed 4 June 2021

prevention of abuse,

Contact tracing apps could be used by States for other purposes than what they are designed for, such as enforcing home quarantine obligations, law enforcement, or national security. End-users can also misuse the app by triggering an exposure notification and unnecessarily sending people into quarantine.

transparency,

Transparency at the very beginning, during, and after the implementation of a contact tracing app enables public oversight, ensures the exercise of the end-user's data protection rights, and promotes public trust. In addition to the transparency requirements of the GDPR, transparency is further needed on the app's source code, development process, userbase and cost.

timing/duration,

Measures such as the use of contact tracing apps and the mass processing of personal data should be limited to crises only. The danger exists that the use of contact tracing apps will be automatically normalised without such decisions being substantiated by States.

interoperability,

The effectiveness of contact tracing apps is dependent on their ability to function in various countries or regions. Moreover, this interoperability enables free movement within the EU internal market to travel for work and tourism.

big tech,

In addition, more regulatory attention is needed for the role of big tech companies and for governments holding them accountable in the execution of public tasks.

Insight nine – Key insights from the monitoring framework on the societal impact of the CoronaMelder and other technological solutions

Due to the novelty of TAGs, insights are needed regarding the perceptions of individual users and the actual impact TAGs have on them. Even less clear are the implications for society at large, and the extent to which the reliance on technological solutions will result in the creation of digital divides, structural inequalities, and the threat to individual freedoms. Recent evaluations of the *CoronaMelder* app provided valuable insights into the public's perceptions, showing the central role played by privacy concerns, social norms, and worries about the power relations introduced by TAGs.[27]

To further our understanding of the societal consequences of the government's introduction of TAGs, one of the goals of this project was to create a monitoring framework to help to identify potential problems and undesired side effects for individuals and society in order to inform a public debate on how to respond to these challenges (see section 9). The monitoring framework consisted of a longitudinal survey that covered a period of twelve months. Multiple topics were covered, including the use of and perceptions about TAGs, related concerns, the role of social and moral norms in the acceptance and uptake of TAGs, issues regarding the role of platforms and infrastructure in introducing the *CoronaMelder*, as well as questions regarding the voluntariness of TAGs use and consent in using them (the concrete surveys used and a more detailed overview of results is included in the section 9 and appendix 3).

In general, the monitoring framework shows that while individuals understand that the *CoronaMelder* may have potential benefits for public health by limiting the spread of the disease, functioning as an early

[27] Ministerie van Volksgezondheid Welzijn en Sport et al., 'Eindrapportage CoronaMelder Evaluatie'.

warning system and having societal benefits that positively impact other measures taken in the crisis, they express more concerns than benefits. The vast majority of individuals worry about the impact of TAGs on their privacy, though only a small group was able to specify this concern, referring to e.g., location tracking or the danger of context creep (i.e. migrating a technological solution from its originally intended context into a new context). The majority of respondents were generally concerned about privacy, though unable to point to the source of their concern (which is commonly observed in research on concerns relating to new technologies). Beyond privacy, we distinguished four further categories of concern that arose due to TAGs: 1) long-term concerns about the impact these technologies would have on society, 2) short-term concerns about others (and e.g., unequal treatment), 3) concerns about consequences for individuals, 4) concerns about fraud and the misuse of the technology and 5) concerns about the lack of access to the technology for certain groups. Overall, these benefits and concerns impacted the actual use of the technology as the perception of benefits for public health strongly drove its uptake, while privacy concerns or those about societal consequences substantially lowered it. In fact, social benefits and concerns were more important drivers of behaviour than individual benefits and concerns.

Next to benefits and concerns, the monitoring framework investigated the social and moral pressures experienced in relation to TAGs. Regarding social norms, we investigated both injunctive (what one believes others expect from him/her) and descriptive norms (what one believes others do) and focused on different social actors that are sources of the norm. Looking at the impact of these norms on installing the *CoronaMelder,* injunctive norms significantly and positively impacted installing the app and this impact was stronger with younger individuals. Descriptive norms do not impact the dependent variable. Breaking down the norms into different social actors, the perceptions about the expectations of direct family members and partners were particularly important. Simultaneously, general injunctive norms negatively impacted behaviour—i.e., the perception that the use of TAGs is generally expected created resistance. Overall, the expectations of others were important for the acceptance and use of TAGs, especially for younger individuals. This was in line with the findings on moral and normative obligations—that individuals use TAGs not because they feel obliged to by the state, but due to the moral obligations they perceive towards society.

The monitoring framework also included users of the *CoronaMelder*. This allowed us to investigate the role of consent in the introduction of such technologies from the perspective of the users. Out of the respondents in the survey who installed the app (624), 368 reported having read the privacy policy, 208 did not, and 48 did not know anymore. When installing the *CoronaMelder*, the respondents were not highly cognitively engaged with the consent they were asked for. The result was 68% of respondents did not understand the technical working of the app, 60% did not know that the app data was not automatically shared with the GGD, and 46% were not aware that the app used infrastructure provided by large platforms. Asked in an open question about their understanding of the app, the majority of users were only able to mention notifications or wrongly expected the app to track the phone's location. Reporting to have read the policy did not improve one's understanding of consent. In general, these conclusions raise questions about the correct functioning of consent mechanisms.

Insight ten – Rethinking academic research in times of crisis: research in action

A question for the discussion of the implications of the COVID crisis for the societal role of academia to inform the public, policy and decision makers, in times of crisis and beyond. If the answer is yes, such a role needs to be reflected in the training of future generations of researchers (e.g., more media training) as well as the outputs of academic research and the focus of research evaluations (i.e., less focus on peer reviewed papers as the main measure of academic productivity, more room for considering alternative forms of communication, e.g., via blogs, op-eds, expert meetings, etc.). In other words, a question that academic research and research institutions need to be prepared to answer is whether we need to create ways to better acknowledge and incentivise new forms of ‘academic research in action’. And a question that decision makers need to be better prepared to answer is: as governments are moving more and more to technology-assisted forms of governance (TAGs), how can we facilitate effective transfer of knowledge and the inclusion of all the different disciplinary perspectives that are needed to understand the potential and implications of TAGs in their full technical, societal, economic, ethical and legal complexity.

Moving forward, this project raised another lesson learned, namely regarding the way research funding is structured and creating room to integrate, acknowledge, and adequately remunerate experts who are not part of the core team, but who still invest their time and expertise despite struggling with competing demands for their time. With the growing complexity and role of digital technology as part of a solution to societal problems, there needs to be more flexibility when thinking about and budgeting for new forms of ‘team science’ in the widest sense. But also acknowledging those contributions made outside the traditional criteria of peer-reviewed publications, acquired research funding and delivered keynotes. This is particularly important for younger researchers who have not yet reached tenure.

The following sections are a collection of articles and background documents produced over the course of the project. Sections 3, 4 and 5 are currently being turned into publications in international peer-reviewed journals. The key findings from this project have been presented, among others, at Tilting Perspectives 2021, Tilburg and the Privacy Law Scholars conference 2021.

2 Mapping digital applications for COVID-19[28]

The impact of the Corona virus crisis on economies and societies has been significant as governments around the globe struggle to find solutions to cope. Typical measures employed in the delay and containment phases have involved the practice of social distancing and self-isolation, increased and vigorous personal hygiene, limiting social gatherings and travel, and testing regimes.[29] The Netherlands practised more relaxed measures compared to its European counterparts, with partial lockdown rules as well as adhering to a "1.5-metre society". Many governments heavily favoured the use of digital technologies, particularly contact tracing apps, to supplement existing measures and manage the crisis more effectively and efficiently. More broadly, technology-led solutions have been driving the response by many governments in the Netherlands, Europe and globally.

Digital technologies can be a useful part of the solution to societal challenges. However, it is critical that the development and implementation of technologies uphold the rule of law and democracy, ensure careful consideration of problem identification, acknowledge the limits of such technologies, and fundamentally situate them in a broader socio-technical-economic-context. Technosolutionism can potentially distract, harm, and even exacerbate situations, rather than addressing their root problems, which are often complex and multi-layered.[30]

Contact tracing apps are a prime example of the risks of technosolutionism, as these apps have been the digital technology of choice by many governments since the start of the outbreak. Due to many concerns raised by NGOs, civil society and academia, many European countries have decided to proceed with contact tracing apps that adopt the decentralised (DP-3T protocol) approach.[31] The involvement of Apple and Google in the development of contact tracing apps and the preceding debates between Member States and the two companies lay bare the EU's dependency and reliance on U.S. technology companies. The dominant gatekeeping positions these companies hold is evident and the ability to leverage their position through setting the terms and conditions of engagement during a public health crisis reflects their power and control over (un)democratic decision-making. It also reflects the uneasy tension between achieving the public objectives of governments and the strategic interests of commercial entities.[32]

Aside from contact tracing apps, the use of digital technologies to manage the COVID-19 crisis must begin by understanding the problems that societies seek to solve. This report identifies four areas of concerns that the Dutch government seeks to address through the use of digital technologies:

[28] The research for this section was concluded in January 2021.

[29] R. Kitchin, 'Civil liberties or public health, or civil liberties and public health? Using surveillance technologies to tackle the spread of COVID-19', *Space and Polity*, 0:0 (2020), 1–20, https://doi.org/10.1080/13562576.2020.1770587.

[30] E. Morozov, 'The tech "solutions" for Corona virus take the surveillance state to the next level', *The Guardian*, 2020, http://www.theguardian.com/commentisfree/2020/apr/15/tech-Corona virus-surveilance-state-digital-disrupt; E. Morozov, *To Save Everything, Click Here: The Folly of Technological Solutionism* (New York: Public Affairs, 2013), https://lib.uva.nl/permalink/31UKB_UAM1_INST/gq32c0/alma990034664970205131.

[31] European Commission, 'Mobile applications to support contact tracing in the EU's fight against COVID-19: Progress reporting June 2020', 2020, https://ec.europa.eu/health/sites/health/files/ehealth/docs/mobileapps_202006progressreport_en.pdf.

[32] N. Appelman et al., 'The Netherlands: Techno-optimis and solutionism as a crisis response', in L. Taylor et al. (eds), *Data Justice and COVID-19: Global Perspectives* (London: Meatspace Press, 2020), pp. 190–97, https://shop.meatspacepress.com/product/data-justice-and-COVID-19-global-perspectives-donate-download.

Table 1. Mapping the areas of concerns to technological domains

	Areas of concerns	Technology domains
1.	To efficiently detect and contain the spread of infections (through identification/detection, self-reporting mechanisms and alerts)	Diagnostic
2.	To continuously assess the situation through evidence and information gathering	Evidence and policymaking
3.	To ensure that society can continue functioning in terms of work and study	Remote productivity
4.	To effectively uphold existing (and new) precautionary and contingency measures through policy and law enforcement	Law and policy enforcement

For governments to be able to navigate these choices and decide on which technological solutions to invest in (or not), substantive debate surrounding the use and deployment of these technologies is needed. This is because the same technology can be used for very different purposes, depending on the objectives and rationale supporting the decision. Contact tracing apps, for example, have demonstrated the need for (and lack of) an assessment framework that can help guide these decisions. Part of such an assessment framework requires mapping the different pros and cons of potential technological solutions, but also providing a better general grasp of the affordances of digital solutions.

This research contributes to forming an assessment framework for the adoption of new digital applications during a public health crisis by providing a discussion of the four domains and offers several examples of digital technologies that have been discussed in this context. This part of the report systematically maps the problems, concerns, expectations and digital technologies used as part of the COVID-19 exit strategy, by (preliminarily) delineating four domains that can systemically address the main concerns as highlighted above: (1) diagnostic, (2) evidence and information gathering, (3) remote productivity, and (4) policy and law enforcement. It provides insights from the lessons learned from the ongoing debates and developments so far of what the problems, concerns and expectations are vis-à-vis technological solutions addressing these four domains. The goal is not to provide a complete overview of all the digital technologies used in the COVID-19 pandemic but rather to identify the digital technologies being debated and used in the Netherlands, and by extension, in Europe and the rest of the world.

2.1 Methodology

In order to systematically conduct this research, we mapped the digital technologies used as part of the COVID-19 exit strategy, categorizing them across four different domains. The first step towards developing this typology was to conduct a literature review on existing digital technologies associated with managing the COVID-19 exit strategy. Conducting this literature review consisted of academic journal articles, news media reports, and grey literature. We reviewed early categorizations of digital COVID-19 applications developed by the European Data Protection Supervisor,[33] academic research,[34] and the European Parliament Research Service,[35] identified overlapping categories, and on that basis developed four main categories. Throughout this investigation, we continued to evaluate these categories when new types of applications became more prominent in the public debate, but this did not lead to changes in the four categories we developed.

[33] W. Wiewiórowski, 'Exchange of views with the LIBE Members on the use of personal data in the fight against COVID-19' (European Data Protection Supervisor, 2020), p. 2, https://edps.europa.eu/sites/edp/files/publication/20-05-07_ww_libe_introductory_remarks_en.pdf.

[34] J. Bullock et al., 'Mapping the landscape of artificial intelligence applications against COVID-19', *ArXiv:2003.11336 [Cs]*, 2020, http://arxiv.org/abs/2003.11336 [accessed 30 June 2020]; U. Gasser et al., 'Digital tools against COVID-19: taxonomy, ethical challenges, and navigation aid', *The Lancet Digital Health*, 2:8 (2020), e425–34, https://doi.org/10.1016/S2589-7500(20)30137-0.

[35] M. Kritikos, 'Ten technologies to fight Corona virus' (European Parliamentary Research Service, 2020), https://www.europarl.europa.eu/RegData/etudes/IDAN/2020/641543/EPRS_IDA(2020)641543_EN.pdf.

Within the four categories, we highlighted certain digital technologies that appeared in our literature scan, and as well as those discussed or used in the real world. The added focus on contact tracing apps and telecommunications in the Diagnostic Technologies category and Evidence and Policymaking category were intentional, as these have been the two main developments in the Netherlands of key importance in the debate on the use of digital technologies.

Through this process, overarching themes and issues relating to the use of digital technologies as part of the COVID-19 exit strategy emerged and were identified. Both the typology and overarching themes and issues serve as a basis to inform and support the legal, ethical and empirical research conducted in our larger project. Due to the time sensitivity and evolving nature of the pandemic, our limitations consist of including some sources that are non-peer reviewed. In order to address these limitations, we valorised our typology and observations with a set of experts interviews.

We adopted purposive sampling, in particular, "expert sampling"[36] by conducting an expert group consultation to validate our typology and expand our preliminary mapping of digital technologies and their related societal concerns. We defined experts as academic researchers working on the topic of technology across various relevant disciplines to ensure a good disciplinary spread. Specifically, we identified those who also have been actively involved in the public debate in both the Netherlands and Europe regarding the use of digital technologies (in particular, contact tracing apps) used during the pandemic. This resulted in a list of 13 experts from nine different disciplines: philosophy and ethics, public governance and administration, information law, science and technology studies (STS), computer science, media and communication, privacy engineering, humanities, and law and technology policy.

The format of the expert group consultation was a half day online discussion, that included splitting the group into two smaller break-out rooms and a plenary session, moderated and facilitated by researchers within this project. We asked the experts questions and facilitated discussions that stemmed from the four main objectives of our expert consultation: (1) to validate our category classifications and digital technologies identified within each category, (2) to validate the overarching themes and societal issues that emerged from this process, (3) to identify potential blind spots, (4) to recommend other stakeholders in order to address biases and missing perspectives to be more inclusive. This resulted in a confirmation of our existing typology with some interesting new examples and some additional overarching themes and concerns. Overall, the findings from the literature review and the consultation of experts were used to further develop the overarching themes and issues that emerge from studying the use of digital technologies in the pandemic, which underpins and threads throughout our report.

Thirdly, to further validate the existing findings from the literature review and expert consultation, we set out to conduct stakeholder interviews with other societal and community groups in the Netherlands. The main goal was to address our blind spots to other perspectives that might be missing, in particular, the contact tracing app and general input on other digital technologies. However, due to the ongoing COVID-19 crisis, which put a lot of pressure on organizations and workers, it was difficult finding people who had the time to speak to us. In the end, we talked to only two organizations. We refer to the insights from the two stakeholder interviews throughout the report.

Our mapping and expert validation strategy supports and is bolstered by quantitative methods in the form of longitudinal surveys in another work package that is part of our overall report and findings (see section 9). This empirical component of the study surveys the societal attitudes of the Dutch population toward the digital technologies identified in our typology and the overarching themes and concerns.

[36] I. Etikan, S. A. Musa, and R. S. Alkassim, 'Comparison of convenience sampling and purposive sampling', *American Journal of Theoretical and Applied Statistics*, 5:1 (2015), 1, https://doi.org/10.11648/j.ajtas.20160501.11.

2.2 Diagnostic technologies

2.2.1 Overview

This section addresses diagnostic technologies, in particular, contact tracing apps and self-diagnostic apps, in relation to containment and mitigation measures. It maps out the key actors and considerations and concerns of the proposed mobile applications, alongside other digital tools potentially used to detect and address the spread of the Corona virus. Diagnostic technologies can broadly be classified as digital tools that range from identification, detection, and self-reporting methods and alerts, as well as those aiding in manual contact tracing efforts. The consensus globally is that contact tracing remains key to coping with the pandemic.[37]

In the Netherlands, the government has been seeking ways to improve its existing efforts in managing the crisis, with the goal of preventing a second Corona wave.[38] The Consultation on the Temporary Act[39], a successful control strategy, contains three main points: (1) testing, (2) tracking, and (3) home reporting. Hence, there appears to be a consensus amongst the government and public authorities that digital tools would greatly supplement existing strategies, as current efforts in manual source and contact tracing were said to be labour intensive and time-consuming. There are also concerns regarding the ineffectiveness of manual tracing, in terms of the number of reports needed to be processed, as well as the inaccuracy or lack of information provided by people who tested positive for COVID-19.[40] The belief is that digital technology will make source and contact tracing more effective and efficient, thus breaking the chain of infections and preventing the further spread of the virus. Certainly, there could be potential usefulness for software applications, such as apps, to aid manual contact tracing, due to the relatively long disease incubation period and the asymptomatic spread of the virus. Apps are also scalable and easily deployable to complement the manual systems of information gathering and notification systems.

However, the effectiveness debate over digital contact tracing apps is still inconclusive. The widely circulated threshold from an Oxford University study for the app to be effective states that at least 56% of the population (approximately 10 million Dutch residents) were required as active users.[41] Yet lower rates of adoption do not necessarily mean the apps are ineffective.[42] The Oxford study clarifies that a lower number of users is also expected to make an impact and decrease infections and the number of deaths. However, on 19 August, a systemic review published in the Lancelet analysing 110 studies concluded that there was no empirical evidence of the effectiveness of automated contact tracing.[43]

Our own surveys and other empirical research show that the main barriers to the adoption of contact tracing apps include concerns over security, privacy and overall public trust in the government[44]. In the case of the Australian contact tracing app, for example, insufficient transparency, inadequate public communication, and legal uncertainty played significant factors in its initial failure.[45] If rates of adoption

[37] World Health Organization. 'Contact tracing in the context of COVID-19,' WHO. 1 February 2021, https://www.who.int/publications/i/item/contact-tracing-in-the-context-of-COVID-19

[38] NL Times. 'Corona virus app tested in Twente region next month,' NL Times, 25 June 2020, https://nltimes.nl/2020/06/25/Corona virus-app-tested-twente-region-next-month

[39] 'Tijdelijke wet notificatieapplicatie COVID-19: Memorie van Toelichting', 2020, sec. 4.2, https://zoek.officielebekendmakingen.nl/kst-35538-3.html.

[40] 'Tijdelijke wet notificatieapplicatie COVID-19: Memorie van Toelichting', 2020, sec. 4.2, https://zoek.officielebekendmakingen.nl/kst-35538-3.html.

[41] R. Hinch et al., 'Effective configurations of a digital contact tracing app: A report to NHSX' (University of Oxford, 2020), p. 12, https://045.medsci.ox.ac.uk/files/files/report-effective-app-configurations.pdf.

[42] P. H. O'Neill, 'No, Corona virus apps don't need 60% adoption to be effective', *MIT Technology Review*, 2020, https://www.technologyreview.com/2020/06/05/1002775/COVID-apps-effective-at-less-than-60-percent-download/.

[43] I. Braithwaite et al., 'Automated and partly automated contact tracing: A systematic review to inform the control of COVID-19', *The Lancet Digital Health*, 2:11 (2020), https://doi.org/10.1016/S2589-7500(20)30184-9.

[44] Public trust in governments have been in decline for many European countries, but trust in both state and central governments in the Netherlands seem to be above average. Edelman Trust Barometer 2020, https://cdn2.hubspot.net/hubfs/440941/Trust%20Barometer%202020/2020%20Edelman%20Trust%20Barometer%20Global%20Report-1.pdf

[45] G. Greenleaf and K. Kemp, 'Australia's "COVIDSafe App": An experiment in surveillance, trust and law', 2020, https://papers.ssrn.com/abstract=3589317.

do not reach the threshold, then other prevention and containment measures have to be stepped up. This is echoed by countries such as Taiwan and South Korea, where it is believed (though unproven), to have helped control and reduce the burden of infection. Countries that have been relatively successful in dealing with the crisis have done so through a combination of strategies, such as extensive testing capacity, imposing strict travel bans, and clear, centralised coordination. Other factors (social, cultural, political, historical), beyond contact tracing apps, are likely to have contributed to their efforts.

In Europe, Iceland has been the most "successful" with the app (if measured by downloads), with 38 per cent of its population having downloaded the app.[46] A high number of downloads, however, does not guarantee active usage. Most adoption rate figures are calculated from the number of downloads and do not take into account the number of uninstalls or active users.[47] In Germany, for example, the app was not working properly for up to five weeks due to a bug that blocked the app from running in the background in order to save power.[48] An app that is not fully functional or difficult to use raises questions about what the drop off rates are, either through deleting the app or having inactive users.

The World Health Organization has issued guidelines stating that there are currently no established methods and metrics for assessing the effectiveness of digital proximity tracking.[49] There are different metrics to calculate the successfulness of an app in general[50] and while there can be a high number of app downloads, it does not equate to retaining active users[51]. Hence, one of the main issues with assessing the effectiveness or success of contact tracing apps is a lack of clarity and depth over assessment metrics. Doing so requires situating the use and adoption of digital technologies beyond the concerns of privacy and consent, important arguments that dominate the debate over digital technologies, but these obscure other concerns relating to these technologies. Other considerations relating to digital inequalities, such as the outsourcing of public functions, compatibility with public health measures, and so forth, are issues that should be considered and raised as part of public policymaking that adheres to democratic decision-making processes.

Inconclusive evidence on the effectiveness of contact tracing apps should serve as a caution to governments investing large resources to developing and using these apps. Rather, resources can and should be allocated towards areas that may be costly but are proven to be effective. Successful containment strategies to date (Taiwan, South Korea, Vietnam) have made major investments in proactive public testing, response infrastructure and coordinated, authoritative public testing,[52] all of which are crucial components in an effective response.[53] Before addressing some of the concerns raised by contact tracing apps, the following will first provide an overview of digital technologies used for diagnosis.

[46] Business Insider US, 'Iceland had the most-downloaded contact-tracing app for its population size. Authorities there say it hasn't made much of a difference,' 12 May 2020, https://www.businessinsider.nl/iceland-contact-tracing-not-gamechanger-2020-5/; France 24, 'Varying degrees of success for Corona virus apps in Europe,' 9 September 2020, https://www.france24.com/en/20200909-varying-degrees-of-success-for-Corona virus-apps-in-europe

[47] P. Dumonteil, 'StopCOVID: L'Application Française de Traçage Parmi les Moins Téléchargées dans le Monde,' BFM TV, 16 July 2017, 2020. https://www.bfmtv.com/tech/stop-COVID-l-application-francaise-de-tracage-parmi-les-moins-telechargees-dans-le-monde_AN-202007160130.html

[48] Deutsche Welle, 'Germany's Corona virus tracing app criticised over warning failures,' *Deutsche Welle*, 25 July 2020, https://www.dw.com/en/germanys-Corona virus-tracing-app-criticized-over-warning-failures/a-54305099

[49] WHO, 'Contact tracing in the context of COVID-19', 2020, https://www.who.int/publications/i/item/contact-tracing-in-the-context-of-COVID-19.

[50] M. Batic, 'What are important mobile app metrics and how to calculate them?', *Medium*, 2019, https://medium.com/datadriveninvestor/what-are-important-mobile-app-metrics-and-how-to-calculate-them-a04de097b0a0.

[51] App Annie, 'Focus on App Retention,' *App Annie*, https://www.appannie.com/en/academy/engage/focus-app-retention/

[52] S. McDonald, 'The digital response to the outbreak of COVID-19', *Centre for International Governance Innovation*, 2020, https://www.cigionline.org/articles/digital-response-outbreak-COVID-19.

[53] C. J. Wang, C. Y. Ng, and R. H. Brook, 'Response to COVID-19 in Taiwan: Big data analytics, new technology, and proactive testing', *JAMA*, 323:14 (2020), 1341, https://doi.org/10.1001/jama.2020.3151.

Telehealth and telemedicine

Telehealth aims to facilitate remote patient-doctor contact and diagnosis, such as self-diagnosis apps and eHealth programmes. In the Netherlands, one diagnostic technology that has been utilised is a self-diagnosis app, *De Corona Check*, which allows users to enter their symptoms daily and teams of doctors and nurses will respond within 24 hours if they are suspected of having the Corona virus in order to help hospitals cope with an influx of requests.[54] This app was created by Amsterdam hospital (OLVG) and digital platform company, Luscii[55]. It is based on an existing Luscii app, already in use for patients to remotely manage chronic diseases, and now offers remote Corona virus guidance.

The usage of telemedicine in healthcare delivery for chronic care management is not new, and with COVID-19, it appears that this evolution towards eHealth will become increasingly prevalent.[56] One of the key issues that continues to be inadequately addressed is the digital inequalities in this growing sector. There are differences which exist between individuals and social groups in terms of access to technologies, but also in terms of their capacity to obtain benefits from the use of technology.[57] Additionally, the digitally disadvantaged tend to belong to segments of the population that experience greater risk, due to age and socio-economic class, further exacerbated by a lower likelihood to use eHealth services, thereby bearing greater risks during the pandemic.[58]

Wearable sensors to track symptoms

Governments globally have deployed various forms of "wearables" to assist in battling the virus. Worn on the wrist, ankle, or anywhere close to the body, wearable sensors serve different purposes. First, they can use an electronic sensor to collect health information and act as an early warning tool to identify potential infected COVID-19 patients. Wearable sensors such as Fitbit and Apple Watch that monitor physiological parameters also claimed to have the potential in delivering early warning signals of a possible COVID-19 infection.[59] Second, they can be used in proximity tracing, to detect or log people's position relative to one another. Last, they can identify a person's location through triangulating the person's bracelet, mobile phone, or a home beacon, to enforce home quarantine.[60] Some devices utilise a GPS receiver, Bluetooth radio beacons, or even low-tech wrist bands, which, in coordination with other digital technologies, can aid and inform authorities on quarantine enforcement.

The growing consumer market for wearable technology highlights the potential in which the use of wearable sensors to contain the spread of COVID-19 could be normalised. In Hong Kong, anyone arriving at the airport in March 2021 had to wear an electronic wristband and use a mobile application to enforce self-quarantine. Wearable sensors have been used as an alternative, or in tandem with contact tracing

[54] NOS News, 'Corona check-app van OLVG nu door iedereen te gebruiken,' *NOS News*, 21 April 2020, https://nos.nl/artikel/2331180-Corona-check-app-van-olvg-nu-door-iedereen-te-gebruiken

[55] Due to the Coronacrisis, Luscii has expanded to work with hospitals in the United Kingdom and Ghana.

[56] Blignault, Ilse, and Craig Kennedy. 1999. "Training For Telemedicine". *Journal Of Telemedicine And Telecare 5*: 112-114. doi:10.1258/1357633991932793. Khilnani, Aneka, Jeremy Schulz, and Laura Robinson. 2020. "The COVID-19 Pandemic: New Concerns and Connections between EHealth and Digital Inequalities." *Journal of Information Communication and Ethics in Society 18 (3)*: 393–403.

[57] Büchi, Moritz; Festic, Noemi; Latzer, Michael (2018). How social well-being is affected by digital inequalities. *International Journal of Communication:3686-3706*. https://doi.org/10.5167/uzh-167385

Hargittai, Eszter. 2010. "Digital Na(t)Ives? Variation in Internet Skills and Uses among Members of the 'Net Generation.'" *Sociological Inquiry* 80 (1): 92–113.

Beaunoyer, Elisabeth, Sophie Dupéré, and Matthieu J. Guitton. 2020. "COVID-19 and Digital Inequalities: Reciprocal Impacts and Mitigation Strategies." *Computers in Human Behavior* 111: https://doi.org/10.1016/j.chb.2020.106424

[58] Khilnani, Aneka, Jeremy Schulz, and Laura Robinson. 2020. "The COVID-19 Pandemic: New Concerns and Connections between EHealth and Digital Inequalities." *Journal of Information Communication and Ethics in Society 18 (3)*: 393–403.

[59] Seshadri, Dhruv R., Evan V. Davies, Ethan R. Harlow, Jeffrey J. Hsu, Shanina C. Knighton, Timothy A. Walker, James E. Voos, and Colin K. Drummond. 2020. "Wearable Sensors for COVID-19: A Call to Action to Harness Our Digital Infrastructure for Remote Patient Monitoring and Virtual Assessments." *Frontiers in Digital Health* 2. https://doi.org/10.3389/fdgth.2020.00008.

[60] Rodriguez, Katitza, Svea Windwehr, and Seth Schoen. 2020. "Bracelets, Beacons, Barcodes: Wearables in the Global Response to COVID-19." *EFF*. June 15, 2020. https://www.eff.org/deeplinks/2020/06/bracelets-beacons-barcodes-wearables-global-response-COVID-19.

apps, to address the issue of the lack of smartphone usage in older populations.[61] For example, in Singapore, while the Bluetooth token was initially distributed to the elderly, it has now been distributed nationally. These tokens will continuously broadcast rotating identifiers that will be cryptographically connected, by the government, to an individual's ID number.

Major issues surrounding privacy violations and mission creep, such as utilising wearable sensors to enforce quarantine control, becomes increasingly possible with the use of such technologies. It also shows how low-tech devices, when combined with other digital infrastructures, can potentially normalise new forms of surveillance and further intensify surveillance capture. Additionally, the global military wearable sensors market is set to grow significantly due to the impact of COVID-19.[62] Several major military wearable sensor companies also offer consumer-facing products.[63] The literature on surveillance technologies in the military context serves ample warning in showing the ease and fluidity in which mission creep can occur.[64]

Temperature guns

Temperature guns have been deployed to determine access to public or private space, including airports and border control. This practice has increasingly become commonplace as travel has slowly begun opening up. In the Netherlands, taking travellers' temperatures via temperature guns is required prior to boarding the aircraft.[65]

Temperature guns are also used for entry into other public spaces, including leisure or business spaces. These strategies have been applied to various extents across countries such as Hong Kong, Singapore, and Taiwan, but less so in European countries, including the Netherlands. Some restaurants and shops, such as the Apple shop at Amsterdam Centraal, require customers to take their temperature prior to entering the shop or their entry will be denied. In these situations, user agency is low as entry into buildings, shops, workspaces, can be easily denied by security personnel or employers, without any appeals mechanism. However, risks to the storing of data, or repurposing of data is low.

QR codes

Due to the contactless feature of QR codes, this technology, which was first developed in the mid-1990s, has made a return. In the Netherlands, QR codes have been popular in facilitating orders at restaurants, but less so in terms of scanning for entry to public and private spaces. The hotels, restaurants and cafes sector were urged to manually collect personal data instead. In France, the government utilised QR codes in their digital COVID-19 confinement forms and rebranded[66] its contact tracing app by expanding it to include the ability to scan the QR code to notify other users (if tested positive), amongst other features.[67] In other parts of the world, such as Taiwan, Hong Kong and Singapore, the use of QR codes to scan for entry to public and private spaces has been more prevalent.

[61] Asher, Saira. 2020. "TraceTogether: Singapore Turns to Wearable Contact-Tracing COVID Tech." *BBC*, July 4, 2020. https://www.bbc.com/news/technology-53146360.

[62] "Global Military Wearable Sensors Market: COVID-19 Business Continuity Plan." 2020. *Businesswire*. September 8, 2020. https://www.businesswire.com/news/home/20200908005716/en/Global-Military-Wearable-Sensors-Market-COVID-19-Business.

[63] "Global Military Wearable Sensors Market: COVID-19 Business Continuity Plan" 2020. *Bloomberg*. September 9, 2020. https://www.bloomberg.com/press-releases/2020-09-08/global-military-wearable-sensors-market-COVID-19-business-continuity-plan-evolving-opportunities-with-analog-devices-inc-and

[64] O'Neil, Patrick H. 2005. "Complexity and Counterterrorism: Thinking about Biometrics." *Studies in Conflict and Terrorism* 28 (6): 547–66.

Dunn Cavelty, Myriam, and Victor Mauer. 2009. "Postmodern Intelligence: Strategic Warning in an Age of Reflexive Intelligence." *Security Dialogue* 40 (2): 123–44.

[65] "Schiphol." n.d. Schiphol.Nl. Accessed May 31, 2021. https://www.schiphol.nl/en/messages/Corona virus-update.

[66] The app rebranded from StopCOVID to TousAntiCOVID with the effort to move beyond *just* a contact tracing app.

[67] France, Connexion. "France to Offer Digital COVID-19 Confinement Forms." *Connexion France*. April 3, 2021. https://www.connexionfrance.com/French-news/France-to-offer-digital-smartphone-COVID-19-confinement-forms-from-Monday-April-6. Dillet, Romain. 2020. "France Rebrands Contact-Tracing App in an Effort to Boost Downloads." *TechCrunch*, October 23, 2020. http://techcrunch.com/2020/10/22/france-rebrands-contact-tracing-app-in-an-effort-to-boost-downloads/.

The scanning of the QR code can be done in several ways, including utilising a built-in QR code reader in a phone camera, through a specific app, or via a separate token. Similar to temperature guns, visitors can be denied entry into public or private spaces for non-compliance. Often, these measures are enforced by private businesses, which individuals have no ability to refute.

Contact tracing apps, however, have been the choice many governments in Europe, as well as globally, opted for. Scotland initially had reservations about developing a contact tracing app, but eventually followed suit at the end of July 2020. In Europe, the only exception has been Sweden, which has resisted this approach, with no plans to launch a contact tracing app.[68] A temporary ban has also been in place for the Norway contact tracing app (Smittestopp) due to privacy violations.[69] Regardless, a snowball effect seems to have occurred amongst countries – further encouraged and abetted by the EU – which have mimicked each other's actions in developing an app as the go-to digital solution to manage the crisis, without any prior assessment of the necessity and potential effectiveness for this solution.[70] Interestingly, this snowball effect did not seem to have applied with regards to other measures.[71] Due to the popular strategy of utilising contact tracing apps, the following section seeks to address some crucial technical considerations and concerns over these apps.

2.2.2 Focus: Contact tracing apps

Contact tracing apps

The initial development of the contact tracing app in the Netherlands through a process of an "appathon" was highly controversial. This sparked a series of public criticisms which led the government, specifically the Ministry of Health, Welfare and Sport (VWS), to re-evaluate its approach in developing the app.[72] In parallel, Apple and Google both announced their collaboration in developing an exposure notification system API based on Bluetooth technology, a decentralised approach to contact tracing apps, which the Dutch government eventually adopted. Briefly, the app (*CoronaMelder*) remains voluntary (opt-in), and the data is analysed and remains stored on the device.

The development of the *CoronaMelder* app was led largely by the Ministry of Health, Welfare and Sport, but involves other actors as well. The Ministry of Health included other actors in the process, such as hackers and cybersecurity experts (such as the NFIR) to test the security and safety of the app (through "bug bounties"), with discoveries checked by an independent third party. Lastly, and unavoidably, the *CoronaMelder* runs on the operating systems of the two technology giants, Apple and Google. After several delays, it was launched mid-October 2020, with about three million installations.[73] However, technical problems related to security, effectiveness and privacy remain.[74]

[68] Sweden has developed other apps, mainly focused on documenting and mapping symptoms of the population rather than contact tracing apps. One was developed by a non-profit group; another was initially developed in the UK and is now used by a research group at Lund University; and the last, was developed by three main public agencies (Public Health Agency, the National Board of Health and Welfare, and the Swedish Civil Contingencies Agency), in collaboration with industry partners to map the experience of symptoms among the population. The digital tool was completed, but never implemented as it was assessed that it would cause more harm than good to the Swedish population. https://algorithmwatch.org/en/project/automating-society-2020-COVID19/sweden; https://ec.europa.eu/health/sites/health/files/ehealth/docs/mobileapps_202006progressreport_en.pdf

[69] EDPB. "Temporary suspension of the Norweigian COVID-19 contact tracing app," June 22, 2020. https://edpb.europa.eu/news/national-news/2020/temporary-suspension-norwegian-COVID-19-contact-tracing-app_en

[70] European Commission. "How Tracing and Warning Apps Can Help during the Pandemic." October 14, 2020. https://ec.europa.eu/info/live-work-travel-eu/Corona virus-response/travel-during-Corona virus-pandemic/how-tracing-and-warning-apps-can-help-during-pandemic_en.

European Commission. "Corona virus: A Common Approach for Safe and Efficient Mobile Tracing Apps across the EU." March 8, 2021. https://digital-strategy.ec.europa.eu/en/news/Corona virus-common-approach-safe-and-efficient-mobile-tracing-apps-across-eu.

[71] For instance, public debates over the effectiveness of the apps have appeared to be subdued in comparison to the debate over the effectiveness of wearing masks, despite the two issues being technical and complex.

[72] Gellert, Raphaël. 2020. "COVID-19 & Data Protection in The Netherlands: Contact Tracing App and Automated Collection of Location Data" Blogdroiteuropeen.Com. Blog Droit Europeen. July 28, 2020. https://blogdroiteuropeen.com/2020/07/28/COVID-19-data-protection-in-the-netherlands-contact-tracing-app-and-automated-collection-of-location-data-by-raphael-gellert/

[73] RTL Nieuws. "CoronaMelder Nu Ruim 3 Miljoen Keer Gedownload." October 19, 2020. https://www.rtlnieuws.nl/tech/artikel/5191231/Coronamelder-nu-ruim-3-miljoen-keer-gedownload

[74] W. Wierda. "'Door Alle Technische Problemen Wegen Voordelen CoronaMelder Niet Op Tegen Nadelen.'" *Folia*. October 29, 2020. https://www.folia.nl/wetenschap/141299/door-alle-technische-problemen-wegen-voordelen-Coronamelder-niet-op-tegen-nadelen

Digital technologies are complex, tend to generate new risks and can be opaque. The involvement of an increasing number of stakeholders—public authorities and private companies—in the realm of technology development in relation to public health, has introduced new actors to mediating relationships between citizens and their governments. Consequentially, it has become crucial to establish clarity and transparency on which actors have access to the app, the relevant data, and information in order to prevent potential abuse or function creep. Yet, there is a lack of visibility to other groups that have been excluded from the process, particularly in the agenda-setting process. Public debate of the app occurred due to a robust civil society, which includes researchers, activists, and academics. Public sentiment, according to the first wave of our empirical study, has highlighted that despite high awareness of the app, motivation to download it remained low.

2.3 Evidence and policymaking technologies

2.3.1 Overview

Gathering information that can be useful to assess the rapidly changing situation of the Corona virus is key to understanding how measures should be introduced, modified or retracted. There are a variety of digital technologies that are being utilised to gather information, which forms the basis for evidence and information gathering. The use of data for evidence gathering is not new. In recent years, technology companies have eagerly leveraged their positions to experiment during humanitarian crises.[75] The challenges of experimentation within the humanitarian sector have shown that before working with external companies or utilising these technologies, careful consideration is required.

In Europe, the use of telecommunication data has increasingly been discussed amongst countries to tackle the pandemic. For example, European Commissioner Thierry Breton has called for EU telecommunication providers to provide mobility and location data to combat the pandemic through population monitoring and tracking infection spread. As such, many telecommunication providers and EU member states have been exploring several private-public partnerships. French telecom operator Orange is repurposing its geolocation service, 2013 Flux Vision, allowing cities to visualise travel flow.[76] Vodafone has committed to helping governments in Europe gain insight into population movements in affected areas, including the development of heatmaps that utilise aggregated and anonymous data, which has been another tool to help authorities better understand population movements.[77]

Data generated and collected on calls include a wide range of meta data (including categories of data that are provided or withheld; metadata includes the identity of each subscriber, recipient or initiator of each call, payments made on the account, and geolocation information). These types of metadata are less valuable for health purposes, but useful for intelligence and police agencies for enforcement purposes. For instance, when O2 shares data with the UK government, or when Swisscom notifies the Swiss authorities of mass gatherings, the purpose is to aid the monitoring and enforcement of social distancing.[78]

While telecommunications data can potentially be useful to gather evidence and information to understand population movement, it can also be used for other purposes such as enforcement of self-quarantine, where the authorities can be alerted of an individual's movements. Viewing this from the lens of enforcement, rather than healthcare, illustrates why governments such as Israel utilised an emergency law

[75] Sandvik, Kristin Bergtora, Katja Lindskov Jacobsen, and Sean Martin McDonald. 2017. "Do No Harm: A Taxonomy of the Challenges of Humanitarian Experimentation." *International Review of the Red Cross* 99 (904): 319–44. doi:10.1017/S181638311700042X

[76] La Quadrature du Net. "Orange Recycles Its Geolocation Service for the Global Pandemic." March 31, 2020. https://www.laquadrature.net/en/2020/03/31/orange-recycles-its-geolocation-service-for-the-global-pandemic/

[77] Vodafone. "Countering the Impacts of the COVID-19 Outbreak." March 18, 2021. https://www.vodafone.com/news-and-media/vodafone-group-releases/news/vodafone-launches-five-point-plan-to-help-counter-the-impacts-of-the-COVID-19-outbreak

[78] Privacy International. "Telecommunications Data and COVID-19." n.d. https://privacyinternational.org/examples/telecommunications-data-and-COVID-19

to include mobile data sharing with its internal security agency,[79] and why it is prone to misuse by being extended beyond its stated purpose.

Telecommunication providers are only one example. The perception of data's value in managing the pandemic extend beyond telecommunications data to location data, which has also been leveraged by other actors, other than telecommunication providers. Other sources of location data are being collected by internet companies and through other means (such as apps). Companies such as Google (i.e., search results for flu trends), Apple and Facebook have leveraged their existing location data sets and offered them to governments, non-profits, and researchers. Therefore, prior to addressing some concerns raised by telecommunication data, the next section will first provide an overview of other forms of digital technologies that are being used for evidence gathering and policymaking.

Sewage testing

In the Netherlands, the RIVM has been conducting research in testing sewage water for traces of COVID-19 since February 2020.[80] The idea is that monitoring virus levels via testing sewage water and stool samples can allow the government to gain better insight into existing infections across municipalities, act as an early warning system, ang gain a better understanding of contamination in the longer term.[81] This method is termed "wastewater surveillance," which gained prominence in the 1990s to eradicate polio and has increasingly become a supplementary action in dealing with COVID-19.[82] Other countries in Europe and other parts of the world have also expanded their use of sewage sampling.[83] These developments often require collaboration with governments, municipalities, water authorities and academic research institutions.

Some potential benefits of sewage testing are: its cost-effectiveness, non-invasiveness, anonymity, access to data from people who lack access to healthcare, and the avoidance of certain biases of other epidemiological indicators.[84] Algorithms and artificial intelligence have also propelled research on "algorithm-driven wastewater testing". At MIT, researchers are looking at how "tree-searching" algorithms can dynamically and adaptively select communities to test for infections.[85] Wastewater surveillance can also speed up vaccine deployments to certain areas where upticks are detected.[86]

[79] Lomas, Natasha. 2020. "Israel Passes Emergency Law to Use Mobile Data for COVID-19 Contact Tracing." *TechCrunch*, March 18, 2020. http://techcrunch.com/2020/03/18/israel-passes-emergency-law-to-use-mobile-data-for-COVID-19-contact-tracing/.
Halbfinger, David M., Isabel Kershner, and Ronen Bergman. 2020. "To Track Corona virus, Israel Moves to Tap Secret Trove of Cellphone Data." *The New York Times*, March 16, 2020. https://www.nytimes.com/2020/03/16/world/middleeast/israel-Corona virus-cellphone-tracking.html.
Times of Israel. 2020. "Knesset Passes Law Authorizing Shin Bet Tracking of Virus Carriers until January." *Times of Israel*. July 21, 2020. https://www.timesofisrael.com/knesset-approves-law-authorizing-shin-bet-tracking-of-virus-carriers/

[80] Medema, Gertjan, Leo Heijnen, Goffe Elsinga, Ronald Italiaander, and Anke Brouwer. 2020. "Presence of SARS-Corona virus-2 in Sewage." *BioRxiv*. https://doi.org/10.1101/2020.03.29.20045880.
S. De Vries. 2020. "Netherlands Leads the Way with Nationwide COVID-19 Sewage Testing." *CGTN*. June 21, 2020. https://newseu.cgtn.com/news/2020-07-21/Netherlands-leads-the-way-with-nationwide-COVID-19-sewage-testing-ShzEz63aMg/index.html.

[81] RIVM. "Rioolwateronderzoek," March 8, 2021. https://www.rivm.nl/Corona virus-COVID-19/onderzoek/rioolwater.

[82] Larsen, David A., and Krista R. Wigginton. 2020. "Tracking COVID-19 with Wastewater." *Nature Biotechnology* 38 (10): 1151–53. https://doi.org/10.1038/s41587-020-0690-1.

[83] M. Berger. 2020. "Scientists around the world are turning to feces to track Corona virus outbreaks". *Washington Post*. October 21, 2020. https://www.washingtonpost.com/world/2020/10/21/wastewater-Corona virus-testing-world-outbreaks/

[84] Larsen, David A., and Krista R. Wigginton. 2020. "Tracking COVID-19 with Wastewater." *Nature Biotechnology* 38 (10): 1151–53. https://doi.org/10.1038/s41587-020-0690-1
Rowe, Alexander K., S. Patrick Kachur, Steven S. Yoon, Matthew Lynch, Laurence Slutsker, and Richard W. Steketee. 2009. "Caution Is Required When Using Health Facility-Based Data to Evaluate the Health Impact of Malaria Control Efforts in Africa." *Malaria Journal* 8 (1): 209.
S, De Vries. 2020. "Netherlands Leads the Way with Nationwide COVID-19 Sewage Testing." *CGNT*. July 21, 2020. https://newseu.cgtn.com/news/2020-07-21/Netherlands-leads-the-way-with-nationwide-COVID-19-sewage-testing-ShzEz63aMg/index.html.

[85] Larson, Richard C., Oded Berman, and Mehdi Nourinejad. 2020. "Sampling Manholes to Home in on SARS-CoV-2 Infections." *PloS One* 15 (10). https://doi.org/10.1371/journal.pone.0240007.
Murray, Scott. 2020. "Testing sewage to home in on COVID-19." *MIT News.* October 28, 2020. https://news.mit.edu/2020/testing-sewage-for-COVID-19-1028

[86] Larsen, David A., and Krista R. Wigginton. 2020. "Tracking COVID-19 with Wastewater." *Nature Biotechnology* 38 (10): 1151–53. https://doi.org/10.1038/s41587-020-0690-1

However, there can be exclusionary effects, such as with communities or facilities with decentralised or faulty wastewater treatment systems, such as prisons, universities or certain hospitals.[87] Additional concerns are that testing results can reveal unrelated results, such as concentrations of certain drugs in specific areas, leading to potential overreach of its initial purpose.

The use of other sources of location data and big data analytics

The use of big data, technologies and data analytics to as part of the emergency response to COVID-19 has been a common response for many governments globally. The proliferation of apps and data sources have led to an increasing trend of using location data by repurposing data from apps that people already have installed on their phones, such as Google Maps and Apple Maps. Partnerships with big technology companies such as Apple, Google and Facebook have emerged, with these technology companies taking the opportunities stemming from the crisis to offer their data and data analytics services to governments[88] and universities.[89] Facebook, for example, is actively collaborating with European governments, the World Health Organization and the European Center for Disease Control, by offering a range of tools and resources to access and manage information as well as using their platform to actively source for new data.[90] Through their Data for Good programme, they provide aggregated and anonymised data through licensing agreements. These developments, however, are not new and big technology companies have been laying the foundations and cementing their dependencies with public actors, further entrenching their infrastructural role.

The Data for Good programme was set up to use data to address humanitarian issues, through mapping population movement and providing data platforms, indexes, dashboards, maps, and forecasts. Concerns have been raised over the experimental nature of data modelling in emergency response due to the mismanagement of information, in particular with regards to the Ebola outbreak.[91] Utilising big data to perform analysis on populations has implications on fundamental rights, including privacy, lack of consent and function creep.

Another example is Google Flu Trends[92] developed in 2009, which was one of the first applications of big data in the public health field. It failed in 2013 when it missed forecasting the peak flu season by 140 per cent.[93] This failure was attributed to "big data hubris," a lack of opacity in terms of data, method and algorithms, which made it dangerous to rely on Google Flu Trends for decision-making.[94] In the COVID-19

[87] CDC. 2021. "National Wastewater Surveillance System (NWSS)." Cdc.Gov. March 24, 2021. https://www.cdc.gov /Corona virus/2019-ncov/cases-updates/wastewater-surveillance.html.

[88] Facebook provided aggregated and anonymised data to the University of Pavia in Italy as part of Facebook's Data for Good programme. Luca, Zorloni. 2020. "Il governo userà i big data nell'emergenza Corona virus. A partire da quelli di Facebook," *WIRED IT*. March 17, 2020. https://www.wired.it/internet/regole/2020/03/17/Corona virus-dati-facebook-privacy/?refresh_ce=

[89] Luca, Zorloni. 2020. "Il governo userà i big data nell'emergenza Corona virus. A partire da quelli di Facebook," *WIRED IT*. March 17, 2020. https://www.wired.it/internet/regole/2020/03/17/Corona virus-dati-facebook-privacy/?refresh_ce=
Lyons, Kim. 2020. "Governments Are Using Cellphone Location Data to Manage the Corona virus." *The Verge*. March 23, 2020. https://www.theverge.com/2020/3/23/21190700/eu-mobile-carriers-customer-data-Corona virus-south-korea-taiwan-privacy. https://www.facebook.com/zuck/posts/10111615249124441

[90] Facebook. 2021. "We're collaborating with European governments and organizations to support relief efforts and keep people informed." https://about.facebook.com/actions/europe

[91] S. McDonald. 2016. "Ebola: A Big Data Disaster," CIS Papers. http://cis-india.org/papers/ebola-a-big-data-disaster

[92] Google Flu Trends is a flu tracking system based on utilising search engine query data to track influenza-like illness in a population, thus claiming to produce accurate early estimates of flu prevalence. Ginsberg, Jeremy, Matthew H. Mohebbi, Rajan S. Patel, Lynnette Brammer, Mark S. Smolinski, and Larry Brilliant. 2009. "Detecting Influenza Epidemics Using Search Engine Query Data." *Nature* 457 (7232): 1012–14. https://doi.org/10.1038/nature07634

[93] Lazer, David, Ryan Kennedy, Gary King, and Alessandro Vespignani. 2014. "Big Data. The Parable of Google Flu: Traps in Big Data Analysis." *Science (New York, N.Y.)* 343 (6176): 1203–5. https://doi.org/10.1126/science.1248506

[94] For example, Google's algorithms were particularly vulnerable to certain terms that were unrelated to flu, and with millions of searches being matched with other external datasets, there were bound to be searches that were coincidental, unlikely to be driven by actual flu trends. D. Lazer and R. Kennedy. 2015. "What We Can Learn From the Epic Failure of Google Flu Trends," *WIRED*. January 1, 2015. https://www.wired.com/2015/10/can-learn-epic-failure-google-flu-trends/. More recent research has shown the desire to re-assess the utility of Google Flu Trends. Santillana, Mauricio, D. Wendong Zhang, Benjamin M. Althouse, and John W. Ayers. 2014. "What Can Digital Disease Detection Learn from (an External Revision to) Google Flu Trends?" *American Journal of Preventive Medicine* 47 (3): 341–47. https://doi.org/10.1016/j.amepre.2014.05.020

pandemic, Google has been providing public health officials across the globe with Community Mobility Reports, which consists of aggregated, anonymised insights from their products such as Google Maps.[95]

While privacy concerns are important, new risks and new dependencies are emerging between big tech companies and governments. Critically, governmental functions and responsibilities in the areas of public health are increasingly outsourced or shared with private actors, but without proper accountability mechanisms or democratic debate. Through their hold over existing data infrastructure, private technology companies are moving into infrastructural positions within societies that raise concerns about democracy.[96]

Data platforms to track the spread of the disease

Data platforms have also been used to track the spread of the disease, including the use of Corona dashboards, disease prevention maps and heatmaps. Corona dashboards have been immensely popular with governments and the WHO. The Netherlands's RIVM Corona dashboard illustrates risk maps, various statistical scales and graphs. Facebook's Data for Good programme, for example, has also launched disease prevention maps. The World Bank has utilised it to forecast needs for COVID-19 testing and hospital beds in Spain, while epidemiologists in France and Italy have been using them to identify at-risk communities.[97]

The dashboard, maps, and other data visualisation tools have come to signify how complex problems are depicted, mainly through a display of comprehensive data. The increasing use of these tools raises concerns over a lack of transparency as to how those numbers, analytics and results have been calculated or verified. More significantly, it also signifies granting value attribution to quantification—in particular, the increasing reliance on quantitative data and indicators, as well as an emphasis on metrics, measurements and values attributed to quantitative methods.[98]

2.3.2 Focus: Use of mobility data

Use of telecommunications mobility data

In the Netherlands, the Parliament debated a legislative proposal that would obligate telecommunications providers to share the telecommunications data of Dutch citizens with the National Institute for Public Health and the Environment (RIVM), via Statistics Netherlands (CBS).[99] According to legislative materials, the government had two objectives for using telecommunications data: (1) enabling the continuous assessment of the control measures in force; and (2) enabling the RIVM to proactively inform municipalities, municipal health services and security regions about possible outbreaks, which could lead to the implementation or reintroduction of control measures at the regional or local level. However, it remains debatable whether these objectives are achievable.

The scheme prescribed by the legislative proposal involves, directly or indirectly, all telecommunications providers in the Netherlands, including KPN, Vodafone, Ziggo and T-Mobile. The new bill in debate would oblige telecommunications providers to collect more data about their customers' whereabouts than is

[95] Google. "See how your community is moving around differently due to COVID-19," n.d. https://www.google.com/COVID19/mobility/
A. Lapatinas. 2020. "The effect of COVID-19 confinement policies on community mobility trends in the EU," EUR 30258 EN, Publications Office of the European Union, Luxembourg, 2020, ISBN 978-92-76-19620-4, doi:10.2760/875644, JRC120972.

[96] Plantin, Jean-Christophe, Carl Lagoze, Paul N. Edwards, and Christian Sandvig. 2018. "Infrastructure Studies Meet Platform Studies in the Age of Google and Facebook." *New Media & Society* 20 (1): 293–310. https://doi.org/10.1177%2F1461444816661553

[97] Facebook Data for Good. 2021. "Our Work on COVID-19." 2020. March 23, 2020. https://dataforgood.fb.com/docs/COVID19/

[98] Diaz-Bone, Rainer, and Emmanuel Didier. 2016. "Introduction: The Sociology of Quantification - Perspectives on an Emerging Field in the Social Sciences." *Historical Social Research* 41 (2 (156)): 7–26. https://www.jstor.org/stable/43798480. Nafus, Dawn. 2016. *Quantified Biosensing Technologies in Everyday Life*. MIT Press. Mau, Steffen. 2020. "Numbers Matter! The Society of Indicators, Scores and Ratings." *International Studies in Sociology of Education* 29 (1–2): 19–37. https://doi.org/10.1080/09620214.2019.1668287

[99] 'Tijdelijke wet informatieverstrekking RIVM i.v.m. COVID-19: Voorstel van Wet', 2020, https://zoek.officielebekendmakingen.nl/kst-35479-2.html.

done in the course of normal business, and to share that data—presumptively in anonymised form—with the RIVM, via the CBS. The RIVM would then use the data to gain insight into how groups of citizens move between municipalities, allowing the municipalities, municipal health services and security regions to undertake a more regional or local approach. The belief was that by sharing data on citizens' movements between municipalities, it would be easier to predict the spread of virus.[100] For example, if there was an outbreak in the municipality of Rotterdam, and the data showed that many citizens from Rotterdam recently travelled to the municipality of Amsterdam, the RIVM would be able to warn the authorities in Amsterdam about a possible outbreak. The RIVM compared the scheme to a 'smoke alarm', allowing for the easy detection of viruses.

In order to facilitate the scheme, telecommunications providers must collect, store, use and transmit mobility data on where a smartphone or another mobile device – and therefore, a citizen – has been every hour of every day, broken down within the municipality. The telecommunications providers must also use their customers' mobility data to determine in which municipality their customers lived over the last thirty days.[101] This means that providers must store traffic and location data for this purpose for at least thirty days, probably needing to create a new database to store all this data.[102] While the new bill has an expiration date of a year, telecommunications providers currently do not normally collect, store, use and transmit this data, thus setting a new precedent.

The government is primarily responsible for the scheme, though it does require large cooperation with private telecommunication companies and public authorities and institutions, such as the municipalities and the RIVM. The government has reserved the competence to issue mandatory instructions on important matters, such as how telecommunications providers must use and transmit mobility data.[103] The telecommunications providers have hitherto expressed a mixed response, urging the government to provide a legitimate legal basis.[104] KPN even decided against sharing mobility data with the European Commission because of the associated privacy risks.[105] Citizens do not hold much agency, aside from turning off their mobile devices or leaving them at home.

Telecommunications providers within as well as outside the European Union, such as Orange in France,[106] Vodafone in Italy,[107] and Vodafone in Australia,[108] have been willing to cooperate with public authorities and institutions. For example, the President of the Robert Koch Institute in Germany noted that the Institute had received mobility data from Deutsche Telekom free of charge, though that data is allegedly also available for purchase.[109]

It is unclear if the intended objectives of the use of telecommunications data can be achieved. Further, the implications on citizens' rights to privacy and data protection, as well as the freedom of association and expression must be considered.

[100] Kasteleijn, Nando. 2020. "Zorgen Bij Telecomproviders over Delen van Reisgegevens Met RIVM." *NOS News*. June 24, 2021. https://nos.nl/artikel/2338328-zorgen-bij-telecomproviders-over-delen-van-reisgegevens-met-rivm.html.

[101] Davies, Jamie. 2020. "Telecoms.Com." *Telecoms.Com*. July 3, 2020. https://telecoms.com/505348/dutch-watchdog-warns-against-data-sharing-to-combat-COVID-19/

[102] Kasteleijn. Nando. 2020. "Privacywaakhond: Huidig Wetsvoorstel Telecomdata Delen RIVM Niet Invoeren." *NOS News*. July 3, 2020. https://nos.nl/artikel/2339365-privacywaakhond-huidig-wetsvoorstel-telecomdata-delen-rivm-niet-invoeren.html

[103] https://zoek.officielebekendmakingen.nl/kst-35479-2.html

[104] Kasteleijn, Nando. 2020. "Zorgen Bij Telecomproviders over Delen van Reisgegevens Met RIVM." *NOS News*. June 24, 2021. https://nos.nl/artikel/2338328-zorgen-bij-telecomproviders-over-delen-van-reisgegevens-met-rivm.html.

[105] https://fd.nl/login?state=hRTOSm&session_state=ba823801-e67e-4691-9fea-20b3296ddd45&code=820c9e9b-6410-4079-972c-1e5ccfc3a78b.ba823801-e67e-4691-9fea-20b3296ddd45.ab0218b1-990b-447b-85ae-4c73399ad1a8

[106] La Quadrature du Net. 2020. "Orange Recycles Its Geolocation Service for the Global Pandemic." March 31, 2020. https://www.laquadrature.net/en/2020/03/31/orange-recycles-its-geolocation-service-for-the-global-pandemic/

[107] Vodafone. 2020. "Countering the Impacts of the COVID-19 Outbreak." March 18, 2020. https://www.vodafone.com/news/press-release/vodafone-launches-five-point-plan-to-help-counter-the-impacts-of-the-COVID-19-outbreak

[108] Grubb, Ben. 2020. "Mobile Phone Location Data Used to Track Australians' Movements during Corona virus Crisis." *The Sydney Morning Herald*, April 4, 2020. https://www.smh.com.au/technology/mobile-phone-location-data-used-to-track-australians-movements-during-Corona virus-crisis-20200404-p54h09.html.

[109] Frankfurter Skriptum. 2020. "Corona virus: Deutscher Mobilfunkbetreiber gibt Bewegungsdaten weiter." *Frask.de*. March 18, 2020. https://frask.de/Corona virus-deutscher-mobilfunkbetreiber-gibt-bewegungsdaten-weiter/

2.4 Remote productivity and sectorial technologies

The pandemic has brought massive disruption to all forms of activities, and one critical context is work. Globally, millions globally shifted to working from home in the past few months but working remotely is not possible for every industry. Hence, the effects of disruption are not equally spread over society. For instance, workers in the healthcare sector have been on the forefront in battling the virus. The crisis has also disproportionately affected workers in precarious situations, such as gig workers who are part of the informal economy and have limited access to welfare and social protections.[110]

For those that have shifted from office to home, video/tele-conferencing, a relatively common technological tool utilised in some workplaces prior to the pandemic has seen an exponential uptake across sectors, including universities and offices. Zoom Video Communications, in particular, has seen its software experience an unprecedented surge in use. Its user base has grown rapidly,[111] with an estimated revenue of €1.5bn, tripling from its previous year.[112] Its capitalisation has grown more than IBM.[113]

The pandemic has also forced universities to transfer their physical learning environments to digital settings. Hence, in addition to adopting teleconferencing tools, online proctoring has surfaced as a way to monitor students taking exams. Online proctoring is a fully automated process and method to detect irregularities and fraud by monitoring student behaviour during an exam. While there are some benefits to utilising these tools, which have been quickly adopted to facilitate work and study across different sectors of society, it also reflects the acceleration and re-organisation of work and education.

Some of these remote productivity tools can also be viewed as "workplace surveillance technologies", "monitoring technologies", and "employee surveillance technologies" that can be applied both to workers at home and on-site at the workplace. The term surveillance thus comes with connotations of a loss of autonomy, invasiveness, security, questions of digital inequalities, and new dependencies. These technologies have increasingly been utilised in knowledge sectors, such traders in the finance industry, as well as in labour-intensive fields, such as factory workers.[114] As the pandemic continues, working and studying from home has become the norm. It is therefore critical to better understand the growing landscape of surveillance technologies and related issues to the use of these digital tools.

Teleconferencing tools

Teleconferencing tools have seen a surge in uptake, in particular, Zoom Communications and Microsoft Teams, creating major concerns over security and privacy. Several governments, such as those of Taiwan and Germany, have banned or restricted the official use of Zoom due to major risks and concerns over

[110] International Labour Organisation. 2020. "ILO Monitor: COVID-19 and the world of work. Second edition." April 7, 2020. https://www.ilo.org/wcmsp5/groups/public/---dgreports/---dcomm/documents/briefingnote/wcms_740877.pdf

[111] Zoom ended April 2020 with 265,400 corporate customers, quadrupling from 2019. The Guardian. 2020. "Zoom Booms as Teleconferencing Company Profits from Corona virus Crisis." *The Guardian*, June 2, 2020. http://www.theguardian.com/technology/2020/jun/03/zoom-booms-as-teleconferencing-company-profits-from-Corona virus-crisis.

[112] The Guardian. 2020. "Zoom Booms as Teleconferencing Company Profits from Corona virus Crisis." *The Guardian*, June 2, 2020. http://www.theguardian.com/technology/2020/jun/03/zoom-booms-as-teleconferencing-company-profits-from-Corona virus-crisis.

[113] The profits of these companies illustrate this popularity. Shares in Zoom went up 74% this year, while the S&P 500 was down 21% in the biggest sell-off since the financial crisis of 2008. Zoom's fourth quarter revenue totaled USD 118.3 million, up 78% year-over-year. The company had added 2.22 monthly active users by the end of February 2020, more than the entirety of 2019. Novet, Jordan. 2020. "Zoom Shares Soar after Revenue More than Quadruples from Last Year." *CNBC*. August 31, 2020. https://www.cnbc.com/2020/08/31/zoom-zm-earnings-q2-2021.html.

[114] S. Spezzati. 2020. "With Traders Far From Offices, Banks Bring Surveillance to Homes." *Bloomberg News*. October 16, 2020. https://www.bloomberg.com/news/articles/2020-10-16/with-traders-far-from-offices-banks-bring-surveillance-to-homes. Hanley, Daniel and Hubbard, Sally. 2020. Eyes Everywhere: Amazon's Surveillance Infrastructure and Revitalizing Worker Power. Open Markets Report. https://static1.squarespace.com/static/5e449c8c3ef68d752f3e70dc/t/5f4cffea23958d79eae1ab23/1598881772432/Amazon_Report_Final.pdf

security and privacy.[115] In the U.S., the videoconferencing platform engaged in deceptive and unfair practices in relation to end-to-end encryption, installing its software without authorisation, thus misleading consumers and placing certain users at risk.[116] Issues of "Zoom bombings" were prevalent across meetings and classrooms, often involving racist and misogynist attacks.[117] The company has yet to publish a transparency report detailing its data security practices, despite attempts from digital rights groups to compel them.[118] Increasingly, these responsibilities over safety in public spaces such as classrooms have been relegated to the trust and safety teams of private actors that are in-charge of determining what is safe (or not) in a classroom environment, which not only creates new vulnerabilities, but also lacks accountability.

Another prominent platform for facilitating teleconferencing is Microsoft. Microsoft Teams, in particular, is included in corporate subscriptions to Office 365 bundle and provides project management, workflow and video conferencing tools. In one week in March, Microsoft Teams users increased by 12 million, from 32 to 44 million, up from 20 million in November.[119] Major concerns over workplace surveillance surfaced in Microsoft 365 regarding workplace analytics.[120] In particular, the Microsoft Productivity Score tool allows for individual level monitoring of workplace productivity across Microsoft suite of tools.[121] Employee behaviour is gathered across 73 metrics, including quantity of emails sent, frequency of contribution to other Microsoft tools, and so forth.[122] Other third parties have been developing more invasive workplace surveillance software and tools, such as tracking keystrokes or inactivity.[123]

However, Microsoft's prominent role across workplaces demonstrates the increasing normalisation of these practices. Data-mining techniques in the consumer sphere has morphed into workplace surveillance the datafication of employment.[124] As such, harvested and logged metadata are reutilised for commercial purposes, such as tools for performance analytics, providing these companies with financially valuable information about their employees. It also introduces new forms of control with barely any checks and balances.

The increased datafication of the workspace and employment through a new range of tools and predictive models, accelerated by the pandemic, will reshape and transform the workplace. Many of these teleconferencing tools apply to varying extents across sectors. This has been prevalent in the gig economy, but also, traditional forms of work are being transformed by the implementation of new data-driven

[115] Wu, Debbie and Illis, Samson. 2020. " Taiwan Bans Official Use of Zoom Over Cybersecurity Concerns." *Bloomberg*. April 7, 2020. https://www.bloomberg.com/news/articles/2020-04-07/taiwan-bans-government-use-of-zoom-over-cybersecurity-concerns. Douglas, Elliot. 2020. " German government restricts use of Zoom over security concerns – reports," Deutche Welle. April 8, 2020. https://www.dw.com/en/german-government-restricts-use-of-zoom-over-security-concerns-reports/a-53069274

[116] Fair, Lesley. 2020. "Zooming in on Zoom's Unfair and Deceptive Security Practices: More about the FTC Settlement. Federal Trade Commission. November 9, 2020. https://www.ftc.gov/news-events/blogs/business-blog/2020/11/zooming-zooms-unfair-deceptive-security-practices-more-about.

[117] Constine, Josh. 2020. "Beware of 'ZoomBombing': Screensharing Filth to Video Calls." *TechCrunch*, March 18, 2020. http://techcrunch.com/2020/03/17/zoombombing/.

[118] Oribhabor, Isedua. 2020. "Open letter: Zoom's policies affecting digital rights." March 18, 2020. *Access Now*. https://www.accessnow.org/cms/assets/uploads/2020/03/Letter-to-Zoom-.pdf

[119] Novet, Jordan. 2020a. "Microsoft Says Teams Communication App Has Reached 44 Million Daily Users." *CNBC*. March 19, 2020. https://www.cnbc.com/2020/03/18/microsoft-teams-app-reaches-44-million-daily-users.html.

[120] Kasana, Mehreen. 2020. "Microsoft 365 Is Going Full Cop on Employees with Constant Monitoring." *Input Mag*. November 25, 2020. https://www.inputmag.com/culture/microsoft-365-is-going-full-cop-on-employees-with-constant-monitoring.

[121] Tung, Liam. 2020. "Microsoft 365's Productivity Score: It's a Full-Blown Workplace Surveillance Tool, Says Critic." *ZDNet*. November 27, 2020. https://www.zdnet.com/article/microsoft-365s-productivity-score-its-a-full-blown-workplace-surveillance-tool-says-critic/.

[122] Stanley, Alyse. 2020. "Microsoft's Creepy New 'productivity Score' Gamifies Workplace Surveillance." *Gizmodo*. November 26, 2020. https://gizmodo.com/microsofts-creepy-new-productivity-score-gamifies-workp-1845763063.

[123] Silverman, Jacob, Melissa Gira Grant, Timothy Noah, Osita Nwanevu, and Christopher Caldwell. 2020. "Do You Know Your Microsoft Productivity Score?" *New Republic*. November 25, 2020. https://newrepublic.com/article/160388/microsoft-productivity-score-workplace-analytics-employee-surveillance.

[124] Adler-Bell, Sam and Miller, Michelle. 2018. "The Datafication of Employment." 2018. *The Century Foundation*. December 19, 2018. https://tcf.org/content/report/datafication-employment-surveillance-capitalism-shaping-workers-futures-without-knowledge/?agreed=1. Sánchez-Monedero, Javier and Dencik, Lina. 2019." The datafication of the workplace". Working Paper. https://datajusticeproject.net/wp-content/uploads/sites/30/2019/05/Report-The-datafication-of-the-workplace.pdf

tools and systems,[125] thereby extending these logistics of surveillance across the spectrum of blue-collared work to white-collared work. As communication tools interact with the wider trend and development of the Internet of Things and the development of machine learning to facilitate the automated processing of information, forms of employee surveillance and performance assessment and management methods will be intensified. These developments will potentially infringe on workers' privacy, as well as exacerbating power asymmetries between workers and employers.[126]

Open-source software

Open-source software has also been used to enforce workplace surveillance. For instance, Amazon's "Distance Assistant" is open-source software that aims at monitoring a worker's distance from other employees to implement real-time social distancing guidelines by providing instant visual feedback when workers are too close to each other (through cameras, TV screens and sensors).[127]

Online proctoring

Online proctoring[128] has become a popular software adopted by universities in order to facilitate examinations. In the Netherlands, some universities have adopted the software of different companies such as Proctorio, ProctorU and Examity. The aim of online proctoring software is to remotely detect fraud during exams based on characteristics of the person or of the room. The system flags fraud based on several elements, such as movement in the workspace, disrupted connectivity and so forth. While universities have provided opt-out options, a choice between opting out of the exam altogether or submitting to proctoring is a risk for many students.

Students across the country have expressed their concerns about the invasive character of online proctoring software.[129] One case was brought forth by the Central Student Council of the University of Amsterdam at the Amsterdam District Court on the grounds of privacy and right to refusal.[130] The Court ruled in favour of online proctoring, however, based on the grounds that Proctorio works in compliance with privacy and data protection regulation.[131]

There are other concerns aside from data protection. Digital inequalities are evident when, for example, students that do not have a stable internet connection or a suitable private home environment, are statistically more likely to be flagged by automated systems.[132] It is unclear if institutions will stop using these systems post-pandemic, or repurpose them in hybrid education formats, with no safeguards or precautions to ensure this will not happen again. As a consequence, online proctoring is emblematic of a shift in education due to the use of digital technologies that have been exacerbated and accelerated by the pandemic. Schools and universities heavily depend on private technology companies to deliver public

[125] Sánchez-Monedero, Javier and Dencik, Lina. 2019." The datafication of the workplace". Working Paper. https://datajusticeproject.net/wp-content/uploads/sites/30/2019/05/Report-The-datafication-of-the-workplace.pdf. Azer, Evronia. 2021. "Remote Working Has Led to Managers Spying More on Staff – Here Are Three Ways to Curb It." *The Conversation*, May 6, 2021. http://theconversation.com/remote-working-has-led-to-managers-spying-more-on-staff-here-are-three-ways-to-curb-it-159604.

[126] Sánchez-Monedero, Javier and Dencik, Lina. 2019." The datafication of the workplace". Working Paper. https://datajusticeproject.net/wp-content/uploads/sites/30/2019/05/Report-The-datafication-of-the-workplace.pdf

[127] Porter, Brad. "Amazon introduces 'Distance Assistant'" Amazon. June 16, 2020. https://blog.aboutamazon.com/operations/amazon-introduces-distance-assistant

[128] Online proctoring can be 'live' or automated. Live proctoring allows a stranger to watch the test taker from inside their home, outsourced and reliant to call centres to be 'live' proctors. Automated proctoring uses facial detection technology and is done using machine learning (here, here).

[129] Univers. 2020. "Online proctoring? Students don't have a real choice." Univers. May 20, 2020. https://univers.wpengine.com/nieuws/2020/05/20/online-proctoring-students-dont-have-a-real-choice/

[130] Konings, Hop and Konings, Han. 2020." Students UvA want to stop webcam-monitored exams." June 2, 2020. *Cursor News at TU/e*. https://www.cursor.tue.nl/en/news/2020/juni/week-1/students-uva-want-to-stop-webcam-monitored-exams/

[131] AT5. "UvA Mag Online Surveillancesoftware Bij Tentamens Blijven Gebruiken." AT5. June 1, 2021. https://www.at5.nl/artikelen/209286/uva-mag-online-surveillancesoftware-bij-tentamens-blijven-gebruiken.

[132] Asher-Schapiro, Avi. 2020. "WHO Looks at Possible 'e-Vaccination Certificates' for Travel," *Reuters*. December 3, 2020. https://www.reuters.com/article/health-Corona virus-who-passports-int-idUSKBN28D1IQ. The QJ Journal. 2020. "Online Proctoring Unfairly Punishes Cheaters & Non-Cheaters Alike." Queensjournal.Ca. Accessed June 4, 2021. Queen's University The QJ Journal. November 20, 2020. https://www.queensjournal.ca/story/2020-11-19/editorials/online-proctoring-unfairly-punishes-cheaters-and-non-cheaters-alike/.

services such as education,[133] and their cloud infrastructures sustain their networks. These dependencies have consequences for the public interest, including allocating public investment into building publicly accessible services and infrastructures, as well as the functioning of universities.[134]

2.5 Law and policy enforcement

A significant discussion on the use of digital technologies to cope with the pandemic revolves around the ability for governments to enforce existing or future policies or instructions related to social distancing or quarantine measures. Several existing technologies that have been utilised for policing, logistics, border control, search and rescue operations, such as facial recognition, drones and thermal scanning, have been repurposed and marketed towards COVID-19 enforcement used in both public and private spaces. Imposing these enforcement controls on the population in democratic societies often requires exceptional permission. Emergencies and crises tend to provide a reason for governments to grant (or not grant) permission through temporary changes in the law. The way that we enable, utilise and check the powers that governments can exert to manage the pandemic, especially facilitated through digitally enabled methods that allow for granularity, will frame a crucial part of governmental power in a world with growing emergencies and uncertainties.[135]

There has been a range of law enforcement mechanisms deployed across many countries globally. Importantly, technology-focused interventions can effectively disable any checks on the governments that deploy and use them as these tools can be wielded with impunity by design. While privacy concerns are valid and important, there are broader issues that surface during an emergency, such as the potential overreach and of abuse of government powers.

In the Netherlands, the use of digital technologies for enforcement purposes has so far remained minimal. New rules and guidelines surrounding the enforcement of the quarantine surfaced in early August, due to increased population movement and a drop in cooperation amongst the population.[136] In August 2020, the Dutch government announced its intentions to tighten quarantine rules by enforcing quarantine measures. Hence, despite the lack of digital enforcement technologies, there should have been careful consideration of whether the usage and deployment of these technologies was actually necessary. Further, many of the technologies that could be used for enforcement purposes would involve and engage private providers, raising questions of potential accountability issues.

Drones for remote communication

Drones have been used to monitor and enforce quarantine compliance and social distancing in Europe and globally. This occurred at the start of the pandemic in countries such as the U.K., Spain, and Greece, where 'shout' drones were deployed, as well as drones capturing footage or images.[137] In China and India, drones were used to disinfect public spaces. Drones have also been used to deliver medical supplies to isolated communities.

[133] In mid-December 2020, Google suffered a global outage across the majority of its services, affecting work, home and educational spaces, including Google Classroom. Hern, Alex. 2020. "Google Suffers Global Outage with Gmail, YouTube and Majority of Services Affected." *The Guardian*, December 14, 2020. http://www.theguardian.com/technology/2020/dec/14/google-suffers-worldwide-outage-with-gmail-youtube-and-other-services-down.

[134] Cribb, Alan, and Sharon Gewirtz. 2013. "The Hollowed-out University? A Critical Analysis of Changing Institutional and Academic Norms in UK Higher Education." *Discourse Studies in the Cultural Politics of Education* 34 (3): 338–50. https://doi.org/10.1080/01596306.2012.717188

[135] McDonald, Sean. 2020. "The Digital Response to the Outbreak of COVID-19." 2020. CIGI Online. March 30, 2020. https://www.cigionline.org/articles/digital-response-outbreak-COVID-19.

[136] NL Times. 2020. "Mandatory Quarantine for COVID-19 Patient's Close Contacts." *NL Times*. August 12, 2020. https://nltimes.nl/2020/08/12/mandatory-quarantine-COVID-19-patients-close-contacts.

[137] Chulvi, Cristina Pauner. 2020. "Drone Use in the Fight against COVID-19 in Spain by Cristina Pauner Chulvi." Blogdroiteuropeen. Com. June 30, 2020. https://blogdroiteuropeen.com/2020/06/30/drone-use-in-the-fight-against-COVID-19-in-spain-by-cristina-pauner-chulvi/. Schippers, Birgit. 2020. "Corona virus: Drones Used to Enforce Lockdown Pose a Real Threat to Our Civil Liberties." *The Conversation*, May 26, 2020. http://theconversation.com/Corona virus-drones-used-to-enforce-lockdown-pose-a-real-threat-to-our-civil-liberties-138058.

However, the human rights implications, as well as the likelihood of continued use, must be assessed.[138] For instance, the human rights implications of drone usage, such as an infringement of privacy due to the lack of consent in being filmed and the duration in which the footage is stored, can occur.[139] Without sufficient safeguards, there are risks that images recorded for health purposes can be re-purposed by law enforcement agencies, enabling these practices to continue even after the crisis. Additionally, Silicon Valley companies have been building closer ties with the military and law enforcement agencies, engaging in private lucrative deals with governments to aid their internal and national security efforts.[140]

Facial recognition and automated distance detection

In public spaces and airports, facial recognition systems, CCTV, and automated distance detection have been deployed to detect individuals experiencing fever, identify individuals that are not complying with certain rules such as mask wearing, or not adhering to social distancing measures. Thermal scanning has been integrated with facial recognition technology, though it has not been not proven to be accurate or effective due to a lack of camera accuracy and the high variance of human temperatures, which might lead to false positives.[141] Additionally, fever detection technology for an asymptomatic nature and/or mild symptoms of the virus (in which a person can be a carrier, even when exhibiting no fever symptoms) does not appear to fully justify its usage.[142]

Despite these considerations, facial recognition technologies are still being widely adopted.[143] As countries seek to open up again, the use of facial recognition technology is set to increase, particularly at airports and train stations.[144] Reports have suggested different growth rates for the global facial recognition technology market—which is likely to be significant in 2021—and the increasing use of private providers for these technologies.[145] While considered a minimally invasive technology compared to traditional biometrics, conceding personal data at such a scale can create new areas of misuse.[146] Increased adoption also raises critical concerns over this technology, such as privacy and security concerns, but also the potential to exacerbate racial and gender biases.[147] Extended use of these surveillance technologies can also lead to chilling effects on societal freedom, even after the pandemic.

[138] In France, the Conseil d'Etat ruled against the use of drones with cameras. Fouquet, Helene and Sebag, Gaspard. 2020. " French COVID-19 Drones Grounded After Privacy Complaint," *Bloomberg News*. 18 May 2020. https://www.bloomberg.com/news/articles/2020-05-18/paris-police-drones-banned-from-spying-on-virus-violators

[139] Schippers, Birgit. 2020. "Corona virus: Drones Used to Enforce Lockdown Pose a Real Threat to Our Civil Liberties." *The Conversation*, May 26, 2020. http://theconversation.com/Corona virus-drones-used-to-enforce-lockdown-pose-a-real-threat-to-our-civil-liberties-138058.

[140] Conger, Kate, and Cade Metz. 2020. "'I Could Solve Most of Your Problems': Eric Schmidt's Pentagon Offensive." *The New York Times*, May 2, 2020. https://www.nytimes.com/2020/05/02/technology/eric-schmidt-pentagon-google.html.

[141] Glaser, April. 2020. "'Fever Detection' Cameras to Fight Corona virus? Experts Say They Don't Work." *NBC News*. March 27, 2020. https://www.nbcnews.com/tech/security/fever-detection-cameras-fight-Corona virus-experts-say-they-don-t-n1170791.

[142] Guariglia, Matthew, and Cooper Quintin. 2020. "Thermal Imaging Cameras Are Still Dangerous Dragnet Surveillance Cameras." Electronic Frontier Foundation. April 7, 2020. https://www.eff.org/deeplinks/2020/04/thermal-imaging-cameras-are-still-dangerous-dragnet-surveillance-cameras.

[143] Van Natta, Meredith, Paul Chen, Savannah Herbek, Rishabh Jain, Nicole Kastelic, Evan Katz, Micalyn Struble, Vineel Vanam, and Niharika Vattikonda. 2020. "The Rise and Regulation of Thermal Facial Recognition Technology during the COVID-19 Pandemic." *Journal of Law and the Biosciences* 7 (1). https://doi.org/10.1093/jlb/lsaa038

[144] Madzou, Lofred. 2020. "Facial Recognition Can Help Re-Start Post-Pandemic Travel. Here's How to Limit the Risks." World Economic Forum. December 16, 2020. https://www.weforum.org/agenda/2020/12/facial-recognition-technology-and-travel-after-COVID-19-freedom-versus-privacy/.

[145] Security World Market. 2020. "Corona virus impacts on facial recognition market," Security World Market. June 11, 2020. https://www.securityworldmarket.com/na/News/Business-News/Corona virus-impacts-on-facial-recognition-market1. Fortune Business Insights. 2020. "Image Recognition Market Size & Share." November 2020. https://www.fortunebusinessinsights.com/industry-reports/image-recognition-market-101855.

[146] Van Natta, Meredith, Paul Chen, Savannah Herbek, Rishabh Jain, Nicole Kastelic, Evan Katz, Micalyn Struble, Vineel Vanam, and Niharika Vattikonda. 2020. "The Rise and Regulation of Thermal Facial Recognition Technology during the COVID-19 Pandemic." *Journal of Law and the Biosciences* 7 (1). https://doi.org/10.1093/jlb/lsaa038

[147] Benjamin, Ruha. 2019. *Race after Technology: Abolitionist Tools for the New Jim Code*. Oxford, England: Polity Press. Zhu, Melissa. 2020. "What Is Facial Recognition, and Why Is It More Relevant than Ever during the Corona virus Pandemic?" *South China Morning Post*. November 6, 2020. https://www.scmp.com/tech/policy/article/3108742/what-facial-recognition-and-why-more-relevant-ever-during-COVID-19.

Immunity passports

With the vaccine being rolled out in December 2020, governments and the travel industry have been keen to develop immunity (or vaccine) passports. In the U.S. these "passports" have been conceived as a form of a digital health pass or digital credential that would include a passenger's testing and vaccine information. This digital document would ideally be managed and verified information between governments, airlines, laboratories and travellers.[148] But linking border control and passport data with personal health data poses many surveillance risks. Estonia started a pilot project in October 2020 with a United Nations health agency to develop a digital vaccine certificate ("e-vaccination certificate") for eventual use in interoperable healthcare data tracking[149], and in the wake of the summer vacation a range of European countries have developed digital passport solutions.

These digital technologies can have significant exclusionary effects. For instance, vaccine distribution is unequal within[150] countries, as well as between countries.[151] Failure to address the issues associated with the availability and affordability of tests and vaccines increases social risk, further marginalising vulnerable groups from protection against the virus. Deployment of these passports can interfere with fundamental rights, including the right to privacy, the freedom of movement and peaceful assembly, and have an impact on equality and non-discrimination.[152]

[148] Gangitano, Alex. 2020. "Airlines Set Sights on Digital Passports for COVID-19 Vaccine." *The Hill*, November 28, 2020. https://thehill.com/policy/transportation/527581-airlines-set-sights-on-digital-passports-for-COVID-19-vaccine.

[149] Miller, John and Nebehay, Stephanie. 2020. "WHO Looks at Possible 'e-Vaccination Certificates' for Travel," *Reuters*. December 3, 2020. https://www.reuters.com/article/health-Corona virus-who-passports-int-idUSKBN28D1IQ.

[150] For example, young children, pregnant women and immunocompromised individuals are advised to wait for further research about the effects prior to taking the vaccine.

[151] Mullard, Asher. 2020. "How COVID Vaccines Are Being Divvied up around the World." *Nature*. https://doi.org/10.1038/d41586-020-03370-6. Twohey, Megan, Keith Collins, and Katie Thomas. 2020. "With First Dibs on Vaccines, Rich Countries Have 'Cleared the Shelves.'" *The New York Times*, December 15, 2020. https://www.nytimes.com/2020/12/15/us/Corona virus-vaccine-doses-reserved.html.

[152] University of Exeter and Economic and Social Research Council. 2020. "Digital Health Passports for COVID-19: Data Privacy and Human Rights Law." Report. https://socialsciences.exeter.ac.uk/media/universityofexeter/collegeofsocialsciencesandinternationalstudies/lawimages/research/Policy_brief_-_Digital_Health_Passports_COVID-19_-_Beduschi.pdf

3 Regulating contact tracing apps for infectious diseases

3.1 Introduction

The spread of communicable diseases can be controlled by a range of containment measures, from vaccines and antiviral medication to non-pharmaceutical interventions, such as the isolation of sick individuals, social distancing, hygiene rules, contact tracing, and home-quarantine.[153] Contact tracing is the process of identifying and informing people that they have been in contact with an infected person.[154] This process aims to break the chain of transmission by finding potentially newly infected individuals and preventing onward transmission.[155] Contact tracing has been used to control sexually transmitted infections, Ebola, and novel infections such as H1N1, SARS, and COVID-19.

Large scale contact tracing done by hand during epidemics or pandemics is challenging and resource intensive. In an interview with public health authorities, an infected person needs to recall their recent contacts and events, after which the authorities reach out to these contacts, inform them of their risk of infection, and advise them to quarantine or take other actions.[156] Infected persons, who might be very ill at the time of the interview, may forget some of their recent contacts or may have been in contact with persons unknown to them, for example, because they used public transport.[157] There are also delays from the moment a person is diagnosed and when their contacts are identified and informed.

Digital technologies can help overcome some of the challenges of contact tracing by hand. Mobile contact tracing applications (“contact tracing apps”) based on proximity tracing can automatically register close contacts, and, once someone is diagnosed, automatically inform these contacts. Some contact tracing apps work on the basis of QR codes that people have to scan with their phone when they enter a space. By the end of 2020, a significant number of EU Member States introduced a contact tracing app for COVID-19.

On an EU level, the European Commission has taken several actions to encourage Member States to develop contact tracing apps and coordinate the different national approaches towards digital contact tracing. Early into the crisis, the Commission adopted a Recommendation on a common Union toolbox for the use of technology and data to combat and exit from the COVID-19 crisis.[158] The Recommenda-

[153] E. Tognotti, ‘Lessons from the History of Quarantine, from Plague to Influenza A’, *Emerging Infectious Diseases*, 19:2 (2013), 254–59, https://doi.org/10.3201/eid1902.120312; M. W. Fong et al., ‘Nonpharmaceutical Measures for Pandemic Influenza in Non-healthcare Settings—Social Distancing Measures’, *Emerging Infectious Diseases*, 26:5 (2020), 976–84, https://doi.org/10.3201/eid2605.190995; J. E. Aledort et al., ‘Non-pharmaceutical public health interventions for pandemic influenza: an evaluation of the evidence base’, *BMC Public Health*, 7:1 (2007), 208, https://doi.org/10.1186/1471-2458-7-208; N. M. Ferguson et al., ‘Strategies for mitigating an influenza pandemic’, *Nature*, 442:7101 (2006), 448–52, https://doi.org/10.1038/nature04795.

[154] ECDC, ‘Contact tracing: Public health management of persons, including healthcare workers, who have had contact with COVID-19 cases in the European Union - first update’, 2020, p. 2, https://www.ecdc.europa.eu/sites/default/files/documents/Public-health-management-persons-contact-novel-Corona virus-cases-2020-03-31.pdf.

[155] ECDC, ‘Contact tracing - first update’, p. 2.

[156] ECDC, ‘Contact tracing - first update’, p. 3.

[157] ECDC, ‘Contact tracing for COVID-19: Current evidence, options for scale-up and an assessment of resources needed’, 2020, p. 4, https://www.ecdc.europa.eu/en/publications-data/contact-tracing-COVID-19-evidence-scale-up-assessment-resources; eHealth Network, ‘Mobile applications to support contact tracing in the EU’s fight against COVID-19: Common EU toolbox for Member States (version 1.0)’, 2020, p. 6, https://ec.europa.eu/health/sites/health/files/ehealth/docs/COVID-19_apps_en.pdf.

[158] ‘Commission Recommendation (EU) 2020/518 of 8 April 2020 on a common Union toolbox for the use of technology and data to combat and exit from the COVID-19 crisis, in particular concerning mobile applications and the use of anonymised mobility data’, https://eur-lex.europa.eu/eli/reco/2020/518/oj.

tion prioritized the development of contact tracing apps and the use of mobility data. The Commission stressed in its Recommendation that Member States should take the development of mobile apps and schemes for using mobility data "as a matter of urgency".[159]

The Commission tasked the eHealth Network to operationalize its Recommendation.[160] The eHealth Network is a voluntary network connecting national authorities responsible for eHealth designated by Member States, established by article 14 of the Cross-Border Healthcare Directive.[161] In the follow-up of the Commission's Recommendation, the eHealth Network adopted, with support of the Commission, among others, the Common EU toolbox for contact tracing apps.[162] The Commission itself also followed up with a Communication about guidance on contact tracing apps in relation to data protection.[163] These various instruments adopted by the Commission and the eHealth Network form an important part of the framework against which we have analysed national approaches towards the regulation of contact tracing apps.

Contact tracing apps may contribute to the protection of public health, which states have a duty to protect. At the same time, they present risks to fundamental rights and societal values, such as equitable access to public health measures and the increased surveillance of the private lives of individuals.[164] It is therefore important to engage in democratic debate about the introduction of contact tracing apps and design legal safeguards for their development and deployment. Legal safeguards also contribute towards ensuring that contact tracing apps are a proportionate measure in protecting public health.[165]

A regulatory framework including at least an explicit legal basis for contact tracing apps may be crucial to ensure that these apps are democratically legitimized. The need for a regulatory framework also follows from the requirement that limitations with fundamental rights should be provided for by law. In other words, we can argue for a legal basis both from the perspective of democratic legitimacy and fundamental rights. In any case, a regulatory framework creates legal certainty about how the app can be used and the (personal) data that is being processed, creating the opportunity to adopt legal safeguards to protect individual rights and restrict new governmental powers.

This chapter assesses the fundamental rights argument for a regulatory framework for contact tracing apps. Thereafter, this chapter considers what regulatory frameworks for contact tracing apps we should address. On the basis of comparative legal research into the few currently existing regulatory frameworks for contact tracing apps in EU Member States and complemented by further fundamental rights analysis, this chapter identifies five key issues that should be regulated: voluntariness, prevention of abuse, transparency, timing/duration, and interoperability. To the extent that current domestic regulatory frameworks do not address these aspects of contact tracing apps, Member States need to adopt new rules, regardless if domestic law already provides for a sufficient legal basis for their app.

This chapter focuses on the question: to what extent should new rules be created? Therefore, this paper discusses the GDPR only to the extent that compliance with this instrument requires the creation of new

[159] 'Commission Recommendation (EU) 2020/518 on a common Union toolbox', para. 2.

[160] 'Commission Recommendation (EU) 2020/518 on a common Union toolbox', para. 6.

[161] 'Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross-border healthcare', https://eur-lex.europa.eu/eli/dir/2011/24/oj; See also, 'Commission Implementing Decision 2019/1765 of 22 October 2019 providing the rules for the establishment, the management and the functioning of the network of national authorities responsible for eHealth, and repealing Implementing Decision 2011/890/EU', https://eur-lex.europa.eu/eli/dec_impl/2019/1765/oj.

[162] eHealth Network, 'Common EU toolbox'.

[163] 'Communication from the Commission: Guidance on Apps supporting the fight against COVID 19 pandemic in relation to data protection', 2020, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020XC0417(08).

[164] A. Lodders and J. M. Paterson, 'Scrutinising CovidSafe: Frameworks for evaluating digital contact tracing technologies', *Alternative Law Journal*, 45:3 (2020), 153–61 (p. 155), https://doi.org/10.1177/1037969X20948262.{\\i{}Alternative Law Journal}, 45:3 (2020

[165] Lodders and Paterson, 'Scrutinising CovidSafe', p. 156.

rules. [166] For example, article 6(1)(e) in conjunction with article 6(3) GDPR requires a legal basis in EU or Member State law, not being the GDPR itself. These provisions may thus call for new rules in case the legal basis does not yet exist for contact tracing apps. Similarly, article 9(2)(i) GDPR requires an EU or Member State's law which provides for suitable and specific measures to safeguard the rights and freedoms of data subjects. We discuss these provisions as they may require the creation of new legal rules. This paper does not discuss the application of the GDPR as such. For example, article 13 GDPR requires that controllers provide certain information to the data subject. Lawmakers do not need to create new rules to ensure compliance with this provision, which means that we do not analyse this provision in this paper. Finally, other relevant legal instruments for contact tracing apps, such as the Medical Devices Directive and the Web Accessibility Directive, are beyond the scope of this research.

3.2 Do contact tracing apps need a new legal basis?

3.2.1 Conditions to limit fundamental rights

Contact tracing apps introduced by EU Member States may interfere with various fundamental rights protected in the EU legal order. The Charter of Fundamental Rights of the EU ("CFEU") protects, among other things, the right to the respect for private and family life (article 7), the right to the protection of personal data (article 8), the right to the freedom of assembly and association (article 12), and the right to the freedom of movement (article 45). Similar to the CFEU, the ECHR protects the right to the respect for private and family life (article 8), the right to the freedom of assembly and association (article 11), and the right to the freedom of movement (article 2 of Protocol 4). The ECHR has derived a right to the protection of personal data from the right to the respect for private life (cite). The right to the freedom of movement is also guaranteed by the founding Treaties of the EU.[167]

The ECHR is relevant for EU Member States for two reasons. The second paragraph of Article 52 of the CFEU states that in so far as the CFEU contains rights which correspond to those guaranteed by the ECHR, the meaning and scope of those rights should be the same as those laid down by the ECHR. Furthermore, all EU Member States are party to the ECHR and thus directly bound to the obligations that follow.

The fundamental rights to the respect for private life, the protection of personal data, the freedom of assembly and association, and the freedom of movement are not absolute rights. Fundamental rights agreements generally contain two systems to restrict certain fundamental rights: limitations and derogations.

Article 15 of the ECHR provides that in times of public emergency and a life-threatening situation for a nation, states may take measures derogating their obligations under the ECHR. The CFEU does not contain a corresponding provision, but the explanations of the CFEU provide that the CFEU does not affect the ability of Member States to use article 15 ECHR. States can use derogations only when normal limitations are insufficient for dealing with an emergency situation.[168]

[166] See on the GDPR and contact tracing apps: K. Bock et al., 'Data Protection Impact Assessment for the Corona App' (Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung, 2020), https://doi.org/10.2139/ssrn.3588172; F. Boehm et al., 'Tracking and tracing apps and data protection in the context of the COVID-19 pandemic: Data protection requirements and recommendations for the deployment of COVID-19 tracking and tracing apps' (FIZ Karlsruhe, 2020), https://www.fiz-karlsruhe.de/sites/default/files/FIZ/Dokumente/FIZnews/tracking_app_EN_20200428.pdf; L. R. Bradford, M. Aboy, and K. Liddell, 'COVID-19 contact tracing apps: A stress test for privacy, the GDPR and data protection regimes', 2020, https://papers.ssrn.com/abstract=3617578 [accessed 21 August 2020]; O. Tambou, 'Data protection issues related to COVID-19 in France part one : issues on health data processing', *blogdroiteuropéen*, 2020, https://blogdroiteuropeen.com/2020/07/23/data-protection-issues-related-to-COVID-19-in-france-part-one-issues-on-health-data-processing-by-olivia-tambou/; O. Tambou, 'Data protection issues related to COVID-19 in France Part 2: Control of some intrusive surveillance by public authorities', *blogdroiteuropéen*, 2020, https://blogdroiteuropeen.com/2020/07/24/data-protection-issues-related-to-COVID-19-in-france-part-2-control-of-some-intrusive-surveillance-by-public-authorities-by-olivia-tambou/.2020

[167] Article 3(2) TEU and article 21 TFEU.

[168] A. Spadaro, 'COVID-19: Testing the limits of human rights', *European Journal of Risk Regulation*, 11:2 (2020), 317–25, https://doi.org/10.1017/err.2020.27.

The system of derogations from fundamental rights it not suitable for the introduction of contact tracing apps. Many EU Member States did not declare a state of public emergency and dealt with the crisis via other legislative competences. During the COVID-19 crisis, states introduced contact tracing apps when the first phase of public emergency was over. For example, the Dutch state presented its contact tracing app as part of its exit strategy from the crisis. In addition, the system of derogations exists to. Therefore, states cannot introduce contact tracing apps by derogating from their obligations to fundamental rights.

Next to the possibility of derogations, states may interfere with fundamental rights on the basis of limiting clauses. The first paragraph of Article 52 of the CFEU provides a general limiting clause. The provision states that any limitation on the exercise of the rights and freedoms recognised by the CFEU must be provided for by law and meet an objective of general interest or the need to protect the rights and freedoms of others. In the ECHR, the provisions that lay down the fundamental rights to respect private life, freedom of assembly and association, and the freedom of movement follow a certain system. The first paragraph of each provision states the fundamental right and the second paragraph (in the case of the freedom of movement: the third paragraph) of each provision provides the limiting clause. Similar to the CFEU, the limiting clauses in the ECHR states that an interference should be provided for by law, which is necessary in a democratic society, and it must be for a legitimate aim. Both the CFEU and ECHR system list the protection of health as a legitimate aim.

From this brief overview, it becomes clear that the CFEU and ECHR require that any interferences with fundamental rights should be provided for by law.

Contact tracing apps, for example, can interfere with the right to data protection. In general, contact tracing apps are designed to reduce the amount of personal data that is processed as much as possible. However, various DPIAs and contact tracing app legislation list several types of personal data that are processed in the context of contact tracing apps, such as the duration that two people are close to each other, the distance they were from each other, the risk score that someone might be infected by the virus, and the IP-address of the end-user.[169] Some people argue that this data are not identifiable and that therefore, contact tracing apps do not process any personal data. However, we cannot exclude the likelihood that contact tracing apps process some personal data. The Explanatory Memorandum to the Dutch contact tracing app legislation also notes that the app was "developed such that the risk of identification is practically impossible. With a view towards maximum care, it is however assumed that there are personal data in all phases of the [contact tracing app".[170]A few pages later, the Explanatory Memorandum says again that "data are almost not traceable".[171] This means that contact tracing apps process (pseudonymized) personal data, albeit in small amounts and with very limited risks of re-identification. Nonetheless, personal data is personal data, and therefore contact tracing apps have to comply with the requirements of the fundamental right to data protection, which means this should be provided for by law. In addition, and depending on the digital solution, contact tracing apps can interfere with other fundamental rights, such as the right to privacy but also the right to the freedom of movement. It is not the purpose of this paper to analyse under which conditions contact tracing apps conflict with fundamental rights but rather to establish whether in the situation that there is a conflict a legal basis is needed.

The ECHR and CJEU have explained in greater detail what the law requirement/condition means. In this regard, it should be noted that the CFEU and ECHR provisions contain slightly different terminology. The CFEU requires that limitations are "provided for by law", whereas the ECHR requires that interferences are "in accordance with the law" or "prescribed by law". However, all these different expressions mean

[169] Article 6d(2)(1) Wet publieke gezondheid.
[170] 'Tijdelijke Wet Notificatieapplicatie COVID-19: Memorie van Toelichting', p. 7.
[171] 'Tijdelijke Wet Notificatieapplicatie COVID-19: Memorie van Toelichting', p. 8.

the same thing.[172] The word "law" should be understood in its substantive sense, not in its formal sense.[173] The word "law" covers written law, also encompassing royal or governmental decrees[174] and regulatory measures taken by professional regulatory bodies under independent rule-making powers delegated to them by Parliament,[175] as well as unwritten law. "Law" includes both statutory law and judge-made law.[176] A law that confers a discretion upon public authorities must indicate the scope of that discretion, although the detailed procedures and conditions to be observed may follow from accompanying administrative practice and do not necessarily have to be incorporated into rules of substance law.[177]

The next issue to consider is whether current law ensures that the introduction of contact tracing apps is provided for by existing law or if new legislation is needed.

3.2.2 Consent in terms of the GDPR to fulfil the provided for by law condition

As explained above, contact tracing apps should be provided for by law. This means that a legal instrument should legitimize the introduction of contact tracing apps by the state. Various Member States argue that specific legislation is not needed because their contact tracing app is based on the (explicit) consent of individuals.[178] These Member States seem to reason that voluntary apps are legitimized because they are based on the provision of (explicit) consent in the GDPR, which consequently meets the condition that interferences with fundamental rights are provided for by law. The Dutch legislature also maintains that consent could form the legal basis,[179] but has nonetheless chosen for another legal ground.

To assess this reasoning, we need to give a brief introduction on the GDPR. The GDPR lays down rules relating to the protection of natural persons with regard to the processing of their personal data.[180] The GDPR applies to the processing of personal data wholly or partly by automated means.[181] Personal data is any information relating to an identified or identifiable natural person.[182] Processing means any operation or set of operations performed on personal data, such as collection, structuring, storage, adaptation, retrieval, use, and disclosure.[183]

As discussed in the previous section, we discuss here the case that contact tracing apps process personal data and thus have to comply with the rules of the GDPR. The GDPR requires that personal data are processed lawfully.[184] Consequently, the GDPR states that the processing of personal data is lawful only if, and to the extent that, one of six legal bases applies, as stipulated in the GDPR.[185] EU lawmakers introduced six legal bases in the GDPR to ensure that any processing of personal data, which constitutes a limitation to the fundamental right to the protection of personal data, is provided for by law (namely: it relies on one of these legal bases) and for a legitimate interest (as specified in the six different legal bases).[186]

[172] ECtHR, The Sunday Times v. the United Kingdom (No. 1), 1979, 6538/74, para. 48, http://hudoc.echr.coe.int/eng?i=001-57584; ECtHR, Silver and Others v. the United Kingdom, 1983, 5947/72; 6205/73; 7052/75; 7061/75; 7107/75; 7113/75; 7136/75, para. 85, http://hudoc.echr.coe.int/eng?i=001-57577.

[173] ECtHR [GC], Leyla Şahin v. Turkey, 2005, 44774/98, para. 88, http://hudoc.echr.coe.int/eng?i=001-70956.

[174] ECtHR, De Wilde, Ooms and Versyp v. Belgium, 1971, 2832/66; 2835/66; 2899/66), para. 93, http://hudoc.echr.coe.int/eng?i=001-57606.

[175] ECtHR, Barthold v. Germany, 1985, 8734/79, para. 46, http://hudoc.echr.coe.int/eng?i=001-57432.

[176] ECtHR, *The Sunday Times v. the United Kingdom (No. 1)*, 6538/74, para. 47.

[177] ECtHR, *Silver and Others v. the United Kingdom*, 5947/72; 6205/73; 7052/75; 7061/75; 7107/75; 7113/75; 7136/75, paras 88–89; ECtHR, Malone v. the United Kingdom, 1984, 8691/79, para. 68, http://hudoc.echr.coe.int/eng?i=001-57533.

[178] European Commission, 'Progress reporting June 2020', p. 9.

[179] 'Tijdelijke Wet Notificatieapplicatie COVID-19: Memorie van Toelichting', p. 15.

[180] Article 1(1) GDPR.

[181] Article 2(1) GDPR.

[182] Article 4(1) GDPR.

[183] Article 4(2) GDPR.

[184] Article 5(1) GDPR.

[185] Article 6(1), first sentence, GDPR.

[186] W. Kotschy, 'Article 6: Lawfulness of processing', in C. Kuner, L. A. Bygrave, and C. Docksey (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press, 2018), pp. 325–26.

The six legal bases in the GDPR are: consent, contract, legal obligation, an individual's vital interests, a public interest task, and the legitimate interests of the controller or third party. However, in the health domain, the six legal foundations to legitimize the processing of personal data are superseded by a prohibition. The GDPR provides that the processing of sensitive personal data, which includes data revealing one's health, is prohibited.[187] There are a few exemptions to this prohibition. The GDPR provides that the prohibition on the processing of sensitive data does not apply if the data subject has given his or her explicit consent.[188]

Contact tracing apps often process "regular" personal data and data concerning health. At first look, one may conclude that "regular" consent and explicit consent may legitimize the processing of personal data in contact tracing apps. However, there are various reasons why, (explicit) consent is not an appropriate legal basis for contact tracing apps introduced by the state to protect public health.

The GDPR defines consent as any freely given, specific, informed, and unambiguous indication of the data subject's wishes.[189] The EDPB has clarified that "free" implies a real choice for data subjects.[190] If the data subject has no real choice, feels compelled to consent, or will endure negative consequences for not consenting, then consent is not valid.[191] Contact tracing apps are introduced in a social and political context that make it hard for individuals to freely give consent to the use of these apps. Our empirical research shows that people feel peer and social pressure to download and use contact tracing apps (see section 9). Furthermore, states present contact tracing apps as part of the effort to end strict containment measures, suggesting that if people do not download the app, their public and personal life may be restricted even longer.[192] The French government, for example, decidedly made use of coercive tactics to convince parliamentarians to support the contact tracing app and to convince citizens to download it.[193] The way in which contact tracing apps are presented to the public thus further increases social pressure.

Some contact tracing apps even promote social pressure. For example, if you download the Dutch contact tracing app, you are presented with a screen that says:

> *Let others know you're helping to stop the Corona virus. The more people who use the CoronaMelder, the better it works. Only together can we stop the spread of the virus. So share the app with as many people as you can.*

In the bottom of the screen, there is a big blue button that allows user to share the app via instant messaging and social media applications on their phone. This big blue button is designed in such a way that it attracts more attention than the button to continue setting up the app without sharing it, thereby further increasing the nudge to share the app.

[187] Article 9(1) GDPR.

[188] Article 9(2)(a) GDPR.

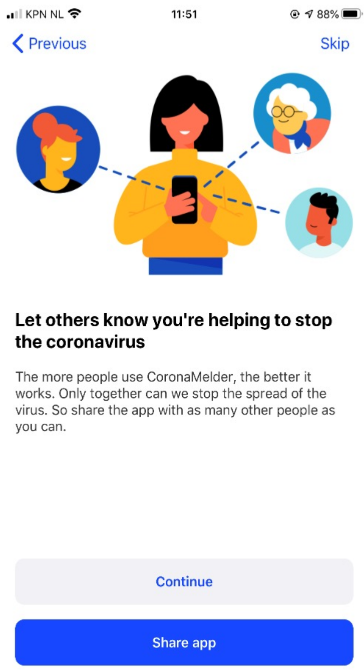
[189] Article 4(11) GDPR.

[190] EDPB, 'Guidelines 05/2020 on consent under Regulation 2016/679 (version 1.1)', 2020, para. 13, https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en.

[191] EDPB, 'Guidelines 05/2020', para. 13.

[192] Bock et al., 'Data Protection Impact Assessment for the Corona App', p. 52; Boehm et al., 'Tracking and tracing apps and data protection in the context of the COVID-19 pandemic', p. 10.

[193] F. Rowe, O. Ngwenyama, and J.-L. Richet, 'Contact-tracing apps and alienation in the age of COVID-19', *European Journal of Information Systems*, 29:5 (2020), 545–62, https://doi.org/10.1080/0960085X.2020.1803155.



Let others know you're helping to stop the coronavirus

The more people use CoronaMelder, the better it works. Only together can we stop the spread of the virus. So share the app with as many other people as you can.

Figure 1.
Screenshot from CoronaMelder App

In addition to social pressure, unequal relationships may also give reason to question if consent can be freely given. The recitals to the GDPR state that where there is a clear imbalance between the data subject and the controller, in particular when the controller is a public authority, it is unlikely that consent was freely given.[194] The EDPB therefore considered that other lawful bases than consent are, in principle, more appropriate for the processing activities of public authorities.[195] The EDPB discusses a few examples to show how the use of consent by public authorities can be appropriate under certain circumstances,[196] but these examples refer to relatively innocuous situations, whereas contact tracing apps are more invasive, creating greater risks for the data subject.

As social pressure and the imbalance of power between citizens and public authorities likely invalidate consent for contact tracing apps, the provisions on consent and explicit consent in the GDPR cannot ensure that contact tracing apps are provided for by law within the meaning of the CFEU and ECHR.

Before we discuss other possible legal grounds for contact tracing apps, it is important to note that the political decision to make contact tracing apps voluntary does not necessarily involve consent as a legal basis. Certain Member States argue that consent is the appropriate legal basis for their contact tracing app because the use of their app by individuals is voluntary and that therefore, additional legislation next to the GDPR is not necessary. However, in its Guidelines on the use of location data and contact tracing tools in the context of the COVID-19 outbreak, the EDPB stresses that "the mere fact that the use of contact-tracing applications takes place on a voluntary basis does not mean that the processing of personal data will necessarily be based on consent."[197] The decision to voluntarily download and use an app is not the same as freely giving informed consent in line with the GDPR, fundamental rights, and democratic principles.

In addition to all these points questioning the legal validity of consent to legitimize contact tracing apps, individual consent might be unsuitable as a governing principle for novel digital applications. As Goldenfein, Green, and Viljoen argue, "[w]hat we need is not *individual control* over data about us, but *collective determination* over the infrastructures and institutes that process data and that determine how it will be used."[198] Processes of democratic law making are one place to exercise such collective determination over digital applications. Therefore, contact tracing apps should be legitimized through a process of democratic law making instead of being legitimized by individual consent, and these apps should be governed by democratically developed legislation—not just by individuals exercising their data protection rights—to ensure these apps serve the public health, not other agendas.

Regardless of whether (explicit) consent can form a legal basis for the processing of personal data in the context of contact tracing apps, to store a contact tracing app on a mobile phone, exchange codes between phones, and upload codes to the back-end server requires consent According to the requirements of article 5(3) ePrivacy Directive. For example, if you download the Dutch contact tracing app, you

[194] Recital 43 GDPR.
[195] EDPB, 'Guidelines 05/2020 on consent under Regulation 2016/679 (version 1.1)', 2020, para. 16, https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en.
[196] EDPB, 'Guidelines 05/2020', paras 17–20.
[197] EDPB, 'Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak', 2020, para. 29, https://edpb.europa.eu/our-work-tools/our-documents/linee-guida/guidelines-042020-use-location-data-and-contact-tracing_en.
[198] J. Goldenfein, B. Green, and S. Viljoen, 'Privacy versus health is a false trade-off', *Jacobin*, 2020, https://jacobinmag.com/2020/04/privacy-health-surveillance-corona virus-pandemic-technology.

have to consent to save the app on your phone and use the functionalities of the API (see also Explanatory Memorandum, p 13). This consent does not relate to the legal basis for contact tracing in terms of the "provided for by law" criterion or the GDPR.

3.2.3 A public interest task to fulfil the 'provided for by law'-condition

If the provisions on (explicit) consent in the GDPR cannot form the legal basis for contact tracing apps introduced by the states and accordingly, cannot fulfil the condition that interferences with fundamental rights should be provided for by law, then states need to establish another legal basis. Next to consent, the GDPR provides that processing of personal data may be lawful if it is necessary for the performance of a task carried out in the public interest, or in the exercise of official authority vested in the controller.[199]

For privacy invasive digital solutions introduced by the state to protect public health or other public interests, the legal basis of a public interest task is most appropriate. In addition to that fact that freely given and informed consent regarding complex digital technologies is difficult to achieve in the relationship between citizens and states, democratic principles require that public authorities operate on the basis of a precise legal framework. In a similar vein, the European Commission[200] and EDPB recommend that contact tracing apps introduced by the state are based on the public interest task, or a legal obligation to which controllers are subject.[201]

As discussed above, in the health domain the six legal bases to legitimize the processing of personal data are overruled by the prohibition on the processing of sensitive personal data, among which are data concerning health. However, the GDPR provides that the prohibition does not apply if the processing of sensitive data is necessary for the purposes of preventive occupational medicine, medical diagnosis, or the provision of health or social care or treatment.[202] In addition, the GDPR provides that the prohibition does not apply if the processing of sensitive data is necessary for reasons of public interest in the area of public health.[203] The EDPB has confirmed that both provisions could apply to contact tracing apps.[204]

The provisions in the GDPR on a public interest task and public health care or medicine create a layered system. The GDPR provides that the public interest task should be laid down by EU or domestic law.[205] The GDPR further provides that the purpose of the processing should be determined in that law or the purpose should be necessary for the performance of the public interest task.[206] Likewise, regarding the special regime for sensitive personal data, the GDPR provides that processing for reasons of medicine, health care, or public health should be based on EU or domestic law.[207] In other words, the GDPR does not create the "real" legal basis for processing for the public interest task and public health care or medicine. Instead, the GDPR expresses that EU or domestic law should provide the legal basis for the processing of (sensitive) personal data for public interest. This means that the GDPR in itself does not yet fully meet the condition that interferences with fundamental rights as posed by contact tracing apps should be provided for by law. Instead, the GDPR mandates that these interferences are provided for by sector-specific EU or domestic law.[208]

[199] Article 6(1)(e) GDPR.

[200] 'Communication from the Commission: Guidance on Apps supporting the fight against COVID 19 pandemic in relation to data protection', para. 3.3.

[201] EDPB, 'Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak', 2020, para. 29, https://edpb.europa.eu/our-work-tools/our-documents/linee-guida/guidelines-042020-use-location-data-and-contact-tracing_en.

[202] Article 9(2)(h) GDPR.

[203] Article 9(2)(i) GDPR.

[204] EDPB, 'Guidelines 04/2020', para. 33.

[205] Article 6(3) GDPR.

[206] Article 6(3) GDPR.

[207] Articles 9(2)(h) and (i) GDPR.

[208] Article 6(3) GDPR also sets forth more specific topics which the EU or domestic law should regulate: "the general conditions governing the lawfulness of processing by the controller; the types of data which are subject to the processing; the data subjects concerned; the entities to, and the purposes for which, the personal data may be disclosed; the purpose limitation; storage periods; and processing operations and processing procedures, including measures to ensure lawful and fair processing". Further discussion of these GDPR requirements is outside the scope of this paper.

3.2.4 Sector specific legislation

Domestic public health law might vest a public interest task or public health care task in the controller and thereby form the legal basis for the processing of personal data by contact tracing apps. In turn, via these laws the condition that interferences with fundamental rights should be provided for by law could be met. The question is if national public health laws indeed create a suitable legal basis in relation to a specific controller. It is outside the scope of this research to analyse all domestic public health laws of EU Member States, but we will analyse the Dutch legal framework to use it as an example.

The Dutch contact tracing app legislation adds a few new temporary provisions to the Dutch public health act[209] and appoints the Minister of Health and the Public Health Service as the app's controllers.[210] The DPIA and Explanatory Memorandum to the legislation state that both controllers may process personal data on the basis of their public interest task.[211] For the Minister of Health, the public interest task is laid down in the Wet publieke gezondheid,[212] which states that the Minister's duty is to advance the quality and effectiveness of public healthcare, maintain and improve the national support structure,[213] and that the Minister leads the combatting of (a serious threat of) an epidemic of communicable diseases of Group A.[214] The Dutch Public Health Service has the public interest duty to perform source and contact tracing for notices of communicable diseases like COVID-19 on the basis of the *Wet publieke gezondheid* (Public Health law).[215]

According to the DPIA and the Explanatory Memorandum to the Dutch contact tracing app legislation, these provisions provide the legal basis for the Dutch contact tracing app.[216] The Dutch *Wet publieke gezondheid* does indeed create a legal basis for contact tracing by the Public Health Service. One could question whether a general provision for contact tracing provides the legal basis for both manual and digital contact tracing. The Explanatory Memorandum to the Dutch contact tracing app legislation argues it does: "Contact tracing has no prescribed form and should be interpreted broadly. The [Dutch Public Health Service] should be able to differentiate according to what is the best approach in certain circumstances."[217] We agree. Similarly, Bradford and colleagues conclude that many national health authorities are sufficiently empowered through domestic public health law to process contact tracing data, even when these data are collected by a mobile app.[218] In contrast, Bock and colleagues conclude that the German *Infektionsschutzgesetz* does not in itself create a legal basis for contact tracing apps by the federal German Public Health Institute.[219]

If we assume that these provisions create a legal basis for digital contact tracing by the Dutch Public Health Institute, then , as the Dutch DPA also remarks, the provisions regarding the Minister of Health do not create a clear legal basis for the processing of personal data with digital contact tracing.[220] The provisions regarding the Minister concern the quality and effectiveness of public health care and the combatting of communicable diseases, but these provisions do not specifically mention contact tracing, neither manual nor digital. Additional legislation needs to be created to establish this legal basis, for example by amending the Dutch *Wet publieke gezondheid*, which the Dutch legislature has indeed done.

[209] A similar system is used in Finland: the law adds temporary chapters to the public health act.
[210] Article 6d(5) and (6) Wet publieke gezondheid.
[211] 'Gegevensbeschermingseffectbeoordeling (DPIA)', 2020, p. 23, https://www.rijksoverheid.nl/onderwerpen/Corona virus-app /documenten/rapporten/2020/07/07/gegevensbeschermingseffectbeoordeling-dpia-COVID-19-notificatie-app.
[212] 'Tijdelijke Wet Notificatieapplicatie COVID-19: Memorie van Toelichting', p. 9.
[213] Article 3(1) Wet publieke gezondheid.
[214] Article 7(1) Wet publieke gezondheid.
[215] Articles 6(1)(c) and 14 Wet publieke gezondheid.
[216] 'Tijdelijke Wet Notificatieapplicatie COVID-19: Memorie van Toelichting', p. 8.
[217] 'Tijdelijke Wet Notificatieapplicatie COVID-19: Memorie van Toelichting', p. 9.
[218] Bradford, Aboy, and Liddell, 'COVID-19 contact tracing apps', p. 12.
[219] Bock et al., 'Data Protection Impact Assessment for the Corona App', p. 57.
[220] Autoriteit Persoonsgegevens, 'Advies op voorafgaande raadpleging COVID19 notificatie-app', 2020, p. 10, https://www.tweedekamer.nl/kamerstukken/detail?id=2020D31782&did=2020D31782.

3.2.5 Interim conclusion

Our interim conclusion is that an interference with fundamental rights should be provided for by law. The GDPR does not create an independent legal basis for contact tracing apps introduced by EU Member States. The legal basis should be laid down in EU or domestic sector specific legislation, such as public health acts. It is beyond the scope of this research to analyse all the domestic public health laws of EU Member States; however, we have analysed the Dutch *Wet publieke gezondheid*, which does not create sufficient legal basis for contact tracing apps. Therefore, to fulfil the "provided for by law" requirement and comply with the GDPR, the Dutch contact tracing app should be accompanied by a newly established law.

The CFEU, ECHR, and GDPR follow more specific requirements regarding what such a legal basis should provide for, such as safeguards against abuse. We will discuss these requirements in the next sections.

3.3 What should contract tracing app legislation regulate at least?

3.3.1 Voluntariness

Contact tracing apps should be voluntary to guarantee the freedom of movement, the freedom of assembly, the integrity of the person, and personal autonomy. [221] Almost all EU Member States which have launched a contact tracing app promised that the use of the app is voluntary, though some governments have toyed with the idea of making such apps mandatory. The Slovenian Prime Minister reportedly called for mandatory contact tracing apps,[222] but after the Slovenian DPA strongly criticized the mandatory use of the app[223] the Prime Minister retracted, saying the app would remain voluntary.[224] The Portuguese government submitted a draft law to the Parliament including a provision that would make the use of the Portuguese contact tracing app mandatory in certain spaces and sectors.[225] However, this provision was criticized and later withdrawn. The European Commission[226] and the EDPB[227] also emphasize that the use of contact tracing apps should be voluntary. The voluntariness of a contact tracing app means that someone who does not want to or cannot use it should not be disadvantaged in any way (beyond the fact that they might miss out on notification warnings) and that people who do use contact tracing apps do not receive certain advantages (aside from the benefits of using the app).[228]

The distinction between voluntary and compulsory apps is a continuum. A legal provision could make an app strictly compulsory. It would be indirectly compulsory when employers, businesses, or public services, such as hospitals, public transport, and universities, would require people to show they have a contact tracing app installed before being allowed to access a building. Furthermore, in social circles, such as among family or friends, people might request others to download the app before visiting. Instead of making an app strictly compulsory, states could use incentives to ensure high uptake.[229] The Lithuanian

[221] U. Gasser et al., 'Digital tools against COVID-19: Framing the ethical challenges and how to address them', *ArXiv:2004.10236 [Cs]*, 2020, pp. 5–6, http://arxiv.org/abs/2004.10236; C. Cattuto and A. Spina, 'The institutionalisation of digital public health: Lessons learned from the COVID-19 app', *European Journal of Risk Regulation*, 11:2 (2020), 228–35 (sec. IV), https://doi.org/10.1017/err.2020.47.

[222] S. Stolton, 'Slovenian PM calls for mandatory Corona virus app, against Commission advice', *Www.Euractiv.Com*, 2020, https://www.euractiv.com/section/digital/news/slovenian-pm-calls-for-mandatory-Corona virus-app-against-commission-advice/.

[223] Informacijski pooblašŞenec, 'Vlada kljub vsemu želi zbirati tudi podatke o naših lokacijah', 2020, https://www.ip-rs.si/novice/vlada-kljub-vsemu-zeli-zbirati-tudi-podatke-o-nasih-lokacijah-1193/.

[224] N. Pirc Musar, 'New powers accorded to the police due to COVID-19 in Slovenia', *blogdroiteuropéen*, 2020, https://blogdroiteuropeen.com/2020/07/28/new-powers-accorded-to-the-police-due-to-COVID-19-in-slovenia-by-natasa-pirc-musar/.

[225] 'Proposta de Lei 62/XIV: Determina a obrigatoriedade do uso de máscara para o acesso ou permanência nos espaços e vias públicas e a obrigatoriedade da utilização da aplicação STAYAWAY COVID', 2020, https://www.parlamento.pt/ActividadeParlamentar/Paginas/DetalheIniciativa.aspx?BID=45409.

[226] 'Communication from the Commission: Guidance on Apps supporting the fight against COVID 19 pandemic in relation to data protection', para. 3.2.

[227] EDPB, 'Guidelines 04/2020', paras 8 and 24.

[228] EDPB, 'Guidelines 04/2020', para. 24.

[229] M. J. Parker et al., 'Ethics of instantaneous contact tracing using mobile phone apps in the control of the COVID-19 pandemic', *Journal of Medical Ethics*, 2020, p. 429, https://doi.org/10.1136/medethics-2020-106314.

app made use of incentives by introducing a gamification element. People received discounts in the app store for using the app and uploading health information. Under those circumstances, an app is not compulsory, but neither is it entirely voluntary. In collaboration with technology companies, states could also push for contact tracing apps being automatically downloaded on all phones, while leaving the option open for people to remove it. The use of the app then becomes a question of opt-in or opt-out. However, in this scenario it might be advisable for states to choose the opt-in action. A study by Altmann and colleagues found that more people would opt-in to an app than keep one that appeared on their phones (the opt-out regime).[230] These examples show that there are multiple ways in which the voluntary nature of a contact tracing app can be put in question. The question is how the law can ensure the voluntariness of an app.

One simple solution to ensure voluntariness is to make it explicit by law. Finnish contact tracing app legislation simply provides that its use is voluntary.[231] However, such a provision is of little value if the legislation does not appoint an entity to enforce it. Data protection authorities are not schooled in how to enforce public health law so this lies outside their capacity. Dutch legislation states that it is prohibited to oblige others to use the contact tracing app or any other similar measure.[232] This prohibition covers gaining access to a building or service, employment, the use of a service, participation in any form of inter-human contact, receiving any kind of advantage conditional on the use of the app or another measure, and the sharing of information from the app or another measure, including whether the user received or did not receive notifications from the app.[233] Such requirements would make the app's use indirectly compulsory. The Dutch legislation qualifies such behaviour as an offence, penalizing it with a fine or six months of detention. Likewise, Belgian,[234] Italian,[235] and Danish legislation provide that the domestic contact tracing app is voluntary.

However, the voluntary nature of the use of an app is affected by various contextual circumstances, such as the installation and uninstallation process and the effects of using or not using the app. Belgian legislation provides a good example of additional provisions to ensure voluntariness. The legislation states that the app should allow users to (temporarily) disable the app and deactivate it and that uninstalling the app should not be more complicated than installing it.[236] In addition, Belgian legislation states that installing, using, and uninstalling the app cannot lead to civil law or criminal law measures, to discriminatory actions, or to any kind of advantage or disadvantage for the end-user.[237]

In the case of contact tracing apps, there are various data processing operations and actions that should each be voluntary. First, downloading the app should be voluntary. Second, sharing one's health status should be voluntary.[238] For example, if someone is diagnosed with COVID-19, they should be able to voluntarily indicate this in the app. It should not be made obligatory to inform others via the app of your health status. The Belgian legislation clearly distinguishes between these two phases. The legislation states that the user should voluntarily relay the fact that they are infected.[239] Third, the EDPB and some national DPAs (such as the Dutch one), argue that the sharing of data with interoperable applications

[230] S. Altmann et al., 'Acceptability of app-based contact tracing for COVID-19: Cross-country survey evidence', *MedRxiv*, 2020, sec. Results, https://doi.org/10.1101/2020.05.05.20091587.

[231] Article 43a Laki tartuntatautilain väliaikaisesta muuttamisesta.

[232] Article 6d(8) Wet publieke gezondheid.

[233] Article 6d(8) Wet publieke gezondheid.

[234] Article 14 §5 Koninkljk besluit.

[235] G. Malgieri, 'The Italian COVID-19 Exposure Alert App: history and legal issues of "Immuni"', *blogdroiteuropéen*, 2020, https://blogdroiteuropeen.com/2020/07/17/the-italian-COVID-19-exposure-alert-app-history-and-legal-issues-of-immuni-by-gianclaudio-malgieri/.

[236] Article 14 § 3(8) Koninkljk besluit.

[237] Article 14 §5 Koninkljk besluit.

[238] EDPB, 'Statement on the data protection impact of the interoperability of contact tracing apps', 2020, para. 5, https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statementinteroperabilitycontacttracingapps_en_0.pdf.

[239] Article 14 §3(11) Koninkljk besluit.

should be voluntary as well.[240] We are not aware of apps that provide people the option to choose to participate in the interoperability framework or legislation that states that participation in the interoperability framework should be voluntary for end-users.

The voluntariness of a contact tracing app also depends on the wider legal system in a given country. In Finland, every person who has or is justifiably suspected of having a generally hazardous or monitored communicable disease is obliged to provide the physician investigating the matter with information regarding the date and place of infection, as well as the names of those who may have been the source of infection of may have been infected.[241] The new provisions on the contact tracing app exempt people who receive information via their app from this obligation.[242]

3.3.2 Prevention of abuse

Contact tracing apps and the data generated by them can be abused by both public and private actors. States can decide to add functionalities to their contact tracing app, for example, turning it into an app used to control home-quarantine obligations. Additionally, public authorities could use the data collected by contact tracing apps for purposes other than public health, such as law enforcement or national security measures. Such function creep does not only happen in authoritarian regimes. For example, in the Netherlands, data about transport, originally collected to inform people about traffic jams, has frequently been used by the Dutch police for criminal investigations.[243] End-users may also abuse contact tracing apps, for example by triggering an exposure notification for other people, forcing them into quarantine.[244]

As discussed above, the European Court of Justice and the European Court of Human Rights require that an interference with fundamental rights is provided for by law. This phrase refers to, among other things, the quality of the law, requiring an interference to be compatible with the rule of law.[245] The requirement of “provided for by law” means that domestic law must contain a measure of protection against arbitrary interferences by the public authorities into fundamental rights.[246] The law should thus provide adequate safeguards against abuse.[247] In addition, the GDPR requires that when health data is processed on the basis of EU or Member State law, this law should provide for suitable and specific measures to safeguard the fundamental rights and interests of the individual.[248]

The next consideration is what specific protections against abuse contact tracing app legislation should contain. It is important to note that design choices and security measures can also protect against abuse of apps and data, in addition to legal rules. For instance, the DP-3T project removed persistent identifiers to prevent states from using contact tracing apps based on a protocol for quarantine control or immunity passports.[249]

[240] EDPB, ‘Statement on the data protection impact of the interoperability of contact tracing apps’, para. 5.

[241] Article 22 Finnish Communicable Diseases Act; English translation: https://finlex.fi/en/laki/kaannokset/2016/en20161227

[242] Article 43d Finnish act.

[243] M. Hijink, ‘Duizenden scanners langs de weg leggen onze gegevens vast’, *NRC*, 26 April 2015, https://www.nrc.nl/nieuws/2015/04/26/duizenden-scanners-langs-de-weg-leggen-onze-gegevens-vast-a1496754.

[244] See more extensively T. Martin et al., ‘Demystifying COVID-19 digital contact tracing: A survey on frameworks and mobile apps’, ArXiv:2007.11687 [Cs], 2020, http://arxiv.org/abs/2007.11687 [accessed 6 September 2020]; R. Anderson, ‘Contact tracing in the real world’, Light Blue Touchpaper, 2020, https://www.lightbluetouchpaper.org/2020/04/12/contact-tracing-in-the-real-world/.

[245] ECtHR, *Malone v. the United Kingdom*, 8691/79, para. 67.

[246] ECtHR, *Malone v. the United Kingdom*, 8691/79, para. 67.

[247] ECtHR, Huvig v. France, 1990, 11105/84, para. 34, http://hudoc.echr.coe.int/eng?i=001-57627; ECtHR, Kruslin v. France, 1990, 11801/85, para. 35, http://hudoc.echr.coe.int/eng?i=001-57626.

[248] Article 9(2)(g) and (i) GDPR.

[249] M. Veale, ‘Sovereignty, privacy and contact tracing’, in L. Taylor et al. (eds), *Data Justice and COVID-19: Global Perspectives* (Meatspace Press, 2020), p. 36, https://shop.meatspacepress.com/product/data-justice-and-COVID-19-global-perspectives-donate-download.

The prevention of function creep by legal rules can be challenging as often the legal and institutional framework adapts to developments and responds to the needs of users of a certain system.[250] Nonetheless, a legal framework can help control function creep. The GDPR contains a set of principles that, if correctly implemented and complied with, would help minimize function creep. The purpose limitation principle requires that personal data are collected for specified purposes and not further processed in a manner that is incompatible with those purposes.[251] According to the EDPB, the sector-specific law that legitimizes processing should specify the purpose and explicitly limit further use of personal data.[252] The data minimisation principle mandates that data processing is limited to what is necessary in relation to the purposes for which the data are being processed.[253] The storage limitation principle requires that personal data are stored for no longer than is necessary for the purposes for which the data were originally collected, unless the data are fully anonymised.[254] Finally, the legal grounds in the GDPR that legitimize data processing all (except for consent) require that data processing is necessary for a given purpose.[255] These principles all contribute to preventing organisations from collecting more data than is truly necessary and repurposing it for other goals.

Ideally, the purpose of a contact tracing app is laid down by law, which also explicitly excludes it being used for other purposes. For example, in Denmark an executive order states that the overall purpose of the contact tracing app is to prevent and deter the spread and transmission of the COVID-19 virus.[256] The executive order explicitly states that Danish Patient Safety Authority may not process the data for other purposes, unless the data is aggregated and anonymised and the processing takes place solely for scientific or statistical purposes.[257]

The data minimisation principle leads to a significant question. The EDPB is of the opinion that contact tracing can be done without tracking the location of individual users and therefore, only proximity data should be used and location data (such as that based on GPS) should not be collected and processed.[258] Furthermore, proximity-based contact tracing apps do not require data on someone's name, health status, and other demographic details, so from the perspective of data minimisation, this data should not be processed. However, some people argue that machine learning-based contact tracing apps are better than "simple" proximity-based apps.[259] Such apps do need to collect more complex user data. Data minimisation and the rules in an accompanying legal framework in which data may be processed by an app therefore depend on which a government chooses as the "best" app.

Several rules make controllers responsible for preventing abuse of apps by end-users and other parties. The GDPR requires that controllers implement appropriate technical and organisational measures to ensure that processing is performed in accordance with the GDPR.[260] This provision should be read together with the principle of integrity and confidentiality, which means that data should be processed in a manner that ensures the security of personal data, including protection against the unauthorised or unlawful processing and destruction or damage of that data.[261]

[250] M. de Vries, 'Hoe waarschijnlijk is function creep? Een wetenschappelijke analyse', in *Function Creep En Privacy* (WODC, 2011), pp. 22–32 (p. 29).
[251] Article 5(1)(b) GDPR.
[252] EDPB, 'Guidelines 04/2020', para. 31.
[253] Article 5(1)(c) GDPR.
[254] Article 5(1)(e) GDPR.
[255] Article 6(1)(b) to (f) GDPR.
[256] Article 1(2) Danish Executive order.
[257] Article 1(4) Danish Executive order.
[258] EDPB, 'Guidelines 04/2020', p. 27.
[259] M. Welling, 'Wees niet bang voor een verdergaande Corona-app', *de Volkskrant*, 20 August 2020, https://www.volkskrant.nl/gs-bb5c35b2.
[260] Article 24(1) GDPR.
[261] Article 5(1)(f) GDPR.

To fulfil these principles and responsibilities, controllers should ensure data protection by design and default.[262] In addition, controllers and processors should implement technical and organisational measures to ensure the security of data.[263]

In addition to technical and organisational measures controllers must take to fulfil their obligations under the GDPR, the GDPR also obliges national lawmakers to adopt legal safeguards. If a contact tracing app involves the processing of data concerning health, and this processing is legitimized by the public interest in the area of public health,[264] then the law should provide for suitable and specific measures to safeguard the rights and freedoms of the data subject.

Some countries have indeed opted to enact legal guarantees against the abuse of data and apps and function creep. In the Netherlands, the legislation states that personal data processed by contact tracing apps should be secured against loss and unlawful processing,[265] and cannot be used for purposes other than combatting the COVID-19 epidemic caused by the COVID-19 virus.[266] Similarly, Finnish legislation states that personal data may be processed only to break COVID-19 infection chains, to inform people about potential exposure, as well as for statistical purposes to monitor the COVID-19 epidemic, and to evaluate the app. But it cannot be used for police, judicial, or other law enforcement purposes.[267] Both Dutch and Finnish legislation thus mainly affirm the purpose limitation principle. However, in the Finnish case, the purpose specification includes the use of data for policy making, which is further developed into a provision stating that some of the pseudonymous data may be transferred to local health authorities and hospitals to assess the measures needed to combat the epidemic.[268] When data collected for digital contact tracing is subsequently used for policy purposes, this risks opening the door to more serious function creep.

Belgian legislation is more detailed. First of all, it protects against data abuse by requiring security, data minimisation, and anonymity measures. The legislation states that the app should enable the user to use an authorisation code to guarantee that only validated information is used and to prevent false, accidental, and mistaken notifications.[269] The legislation also states that the app should guarantee that only information about potential infection and the date on which the individual was infected cannot be tracked down.[270] Second, the Belgian legislation protects against abuse of the data and function creep by regulating how data processing can be stopped. The legislation states that the central database can be deactivated at any time and that the processing of personal data can be (temporarily) ended by a decision of the responsible authority.[271] Furthermore, the legislation specifies that the central database needs to be deactivated when the data are no longer necessary for the exit strategy and that the central database needs to be deactivated after a year,. [272] Third, the legislation states that the contact tracing app and the data processed by it cannot be used for other purposes as specified in the act, in particular law enforcement, commercial, criminal law, or national security purposes.[273] With this mix of measures, Belgian legislation aims to provide broad protection against data abuse and function creep.

The question is how far should legislation go in protecting against data abuse and function creep? For example, the DPIA for the Dutch contact tracing app states that when a user validates their authorisation

[262] Article 25 GDPR.
[263] Article 32 GDPR.
[264] Article 9(2)(i) GDPR.
[265] Article 6d(3)(b) Wet publieke gezondheid.
[266] Article 6d(3)(c) Wet publieke gezondheid.
[267] Article 43c Finnish legislation.
[268] Article 43e Finnish legislation [double check translation!]
[269] Article 14 § 3(6) Koninklijk besluit.
[270] Article 14 § 3(7) Koninklijk besluit.
[271] Article 14 § 3(9) Koninklijk besluit.
[272] Article 14 § 10 Koninklijk besluit.
[273] Article 14 § 7 Koninklijk besluit.

code with the national health service, their phone sends its IP-address to the back-end server, which is unavoidable with the use of internet and IP-technology.[274] Dutch legislation states that the controller should ensure that this IP-address is separated as quickly as possible from other data and stored separately.[275] It also prohibits anyone from connecting this IP-address with other data, including that processed by the contact tracing app.[276] With these rules in place, Dutch legislation tries to reduce the data's traceability by taking into account that the chosen design for the Dutch contact tracing app makes it technically impossible *not* to send the IP-address to the back-end server. However, one could argue that legislation should mandate that the IP-address is immediately deleted,[277] rather than being stored separately.

3.3.3 Transparency

To ensure that end-users can exercise their data protection rights and further enable the public oversight of a contact tracing app, different modes of transparency relating to the app are required. Transparency at the very beginning, during, and after the implementation of a contact tracing app enables the constant monitoring of the legitimacy, necessity, and proportionality of the choice for a certain digital solution by the state in relation to its impact of fundamental rights.[278] Parliaments, journalists, and expert citizens can perform a public watchdog function when the development and implementation of a contact tracing app is made transparent. Next to enabling control and oversight, publishing and sharing the source code and peer reviews of a contact tracing app can promote interoperability.[279] Transparency can also increase the public's trust in a contact tracing app, which can lead to its higher uptake.

Another important consideration is about which aspects of a contact tracing app the government should offer transparency on. The GDPR mandates transparency about a set of issues (purposes, data types, recipients of data—which is especially important for interoperable apps, etc). In addition to what the GDPR mandates, we need transparency concerning the source code of a contact tracing app, and ideally transparency over the Google and Apple API or other operating system components necessary to make a contact tracing app work. Furthermore, we need transparency on an app's development process. Which choices were made and why, and what were the alternatives? To monitor an app's effectiveness and thus assess its necessity, we need transparency about the number of people downloading and activating a contact tracing app, how many people upload their infection status via the app, how many receive warning notifications via the app, and how many receive notification via the app who would otherwise not have been warned via manual contact tracing. Finally, we need transparency about the costs of an app, including its development, communication, and upkeep.

Swiss contact tracing app legislation exempts third parties, that is, Google and Apple, from publishing the source code of their API. Google and Apple did release some details, respectively snippets and sample codes.[280]

Transparency is thus important with regard to different communities, namely individual end-users, DPAs, other supervisory authorities, the Parliament, expert users, the media, and the wider public. Furthermore, transparency involves the concerns of different actors, namely the government as the data controller and developer of the app, Google and Apple as infrastructure providers, and the national health services/ authorities.

[274] 'Gegevensbeschermingseffectbeoordeling (DPIA)', pp. 10–11.
[275] Article 6d(11) Wet publieke gezondheid.
[276] Article 6d(11) Wet publieke gezondheid.
[277] https://twitter.com/lilianedwards/status/1308028969430798336
[278] Spadaro, 'COVID-19: Testing the limits of human rights'.
[279] eHealth Network, 'Common EU toolbox', p. 24.
[280] https://www.esat.kuleuven.be/cosic/sites/Corona-app/wp-content/uploads/sites/8/2020/08/lessons-from-swissCOVID -68c62592bc21099e1d069e8db6694ebf.pdf , p 4.

A legislative process enables transparency. Through discussing the legal basis and the conditions that will be applicable to a contact tracing app in the Parliament, the government can be held accountable for its choice to introduce exceptional measures. A significant issue is that tech companies are not accountable to national Parliaments. Therefore, it is even more important that the agreements governments arrange with tech companies are made public, so that both Parliament and the public can hold the government accountable for these agreements.

In addition, legislation on contact tracing apps should require more transparency. Obligations to publish information about the contact tracing app in open source have been set by several countries, mostly through specific rules in legislation. The Belgian contact tracing app legislation mandates that the full source code of the contact tracing app and the full interface be made public.[281] However, any contact tracing app relying on GAEN will be open source only when Google and Apple also make all aspects of their framework open source, which is not yet the case. See AP (p 8) for more references. This also relates to the previous points about our dependency on Google and Apple. States are reliant on Google and Apple making their frameworks fully open source before they can meet their own open-source obligations or commitments.

Also, although the GDPR does not oblige controllers to publish their DPIA, some countries have chosen to make such an obligation part of their regulatory framework. The EDPB strongly recommends the publication of DPIAs of contact tracing apps.[282] The Belgian contact tracing app legislation requires that the DPIA for the national contact tracing app be made public.[283] British researchers propose that any DPIA should be made public for a consultation period before the system is actually put into operation.[284] Parliamentarians in England also suggest that the DPIA should be made public and updated as digital contact tracing progresses.[285]

3.3.4 Sunset clauses

Crisis measures should apply only during a crisis and not merge into the new normal. Once contact tracing apps have been developed and deployed, and people have been running them in the background of their phones for a while without really thinking about it, there is a risk that governments will no longer be concerned with dismantling the apps and their supporting infrastructures. [thus normalizing surveillance]. Furthermore, the WHO has warned that the COVID-19 virus might become endemic, even once populations are vaccinated.[286] As the crisis continues for months if not years to come, governments may try to legitimize the continued use of digital technologies such as contact tracing apps as the way for societies to live with the COVID-19 virus and possibly extend the use of data generated by contact tracing apps for other (epidemiological) purposes. To ensure that a government needs to substantiate its decision to continue using contact tracing apps and prove their continued effectiveness (which was hard to do at the beginning of the crisis due to a lack of data, but which should be increasingly achievable when apps have been used for longer), the law should ensure that contact tracing app systems are temporary and can be prolonged only through democratic procedure.

In the case of contact tracing apps, there are several components that should have limited duration: the app itself, data stored locally, data stored on the central server, the central server system, and the underlying Google and Apple API. In a press conference, the European Commission has affirmed that contact

[281] Art 14 §3(14) Koninklijk besluit.
[282] EDPB, ‘Guidelines 04/2020’, para. 39.
[283] Art 14 §8 Koninklijk besluit.
[284] L. Edwards et al., ‘The Corona virus (Safeguards) Bill 2020: Proposed protections for digital interventions and in relation to immunity certificates’, 2020, https://doi.org/10.31228/osf.io/yc6xu.
[285] https://publications.Parliament.uk/pa/jt5801/jtselect/jtrights/343/343.pdf
[286] M. Davey, ‘WHO warns COVID-19 pandemic is “not necessarily the big one”’, *The Guardian*, 29 December 2020, section World news, https://www.theguardian.com/world/2020/dec/29/who-warns-COVID-19-pandemic-is-not-necessarily-the-big-one [accessed 29 December 2020].

tracing apps may be used in future public health crises (cite). Furthermore, the Google and Apple API that was downloaded with the OS update potentially creates a new infrastructure for global mass surveillance.[287] In this regard, contact tracing through mobile phones is an unprecedented approach towards protecting public interests, as it turns mobile phones, which people carry for personal or work-related purposes, into public health technologies.

The storage limitation principle in the GDPR requires that data are kept in a form which permits identification of data subjects no longer than is necessary for the purposes for which the personal data are processed.[288] In principle, accompanying new legislation for a contact tracing app does not need to repeat this principle. Some legislatures have still opted to replicate this principle. For example, the Dutch contact tracing app legislation provides that personal data processed in the context of the contact tracing app should not be stored longer than necessary to notify users of a potential infection and should be deleted immediately thereafter.[289] The Explanatory Memorandum to the legislation specifies that the maximum storage time is 14 days and explains that this time period is not based on scientific insight; therefore, storage time might become longer or shorter.[290] In Denmark, the contact tracing app legislation distinguishes between data on the user's phone and data stored by health authorities, specifying that the former should be deleted after 14 days or when the user uninstalls the app,[291] whereas the latter uses different storage periods depending on the type of data.[292]

In addition to the data on someone's phone, for any contact tracing system, some personal data are stored on a central server. In Belgium, the contact tracing app legislation states that data on the central server should be deleted at the latest after 60 days.[293]

We are not aware of a country that has specified a sunset clause for the operation of the Google and Apple API.

Finally, next to personal data and the API, the legislature can specify a sunset clause for contact tracing app legislation and the conditions under which it should be prolonged. If a regulatory framework expires, then the operation of the app is no longer automatically legal, so a sunset clause for the legislation itself also covers the app. Dutch contact tracing app legislation specifies that the new articles will expire three months after the new legislation comes into effect,[294] while the government can prolong the legislation for three months through an executive order.[295] To ensure democratic accountability, Dutch contact tracing app legislation requires a draft executive order to be presented with a week's notice to the Parliament.[296] From a technical point of view, the Dutch app can "self-destruct".

The Dutch DPA advised including an obligation to evaluate the app after a certain amount of time, but the Dutch legislature explicitly chose not to include such a provision in the contact tracing app legislation on the basis of the EDPB opinion, as EU Member States were already instructed to monitor the workings of the app.[297] According to the Dutch legislature, it is clear that use of the app will be ended when it does not contribute to manual source and contact tracing by the Dutch public health service.[298] One could argue that we need more clear and transparent criteria to determine when the app will be ended or

[287] J.-H. Hoepman, 'Google Apple Contact Tracing (GACT): A wolf in sheep's clothes', https://blog.xot.nl/2020/04/19/google-apple-contact-tracing-gact-a-wolf-in-sheeps-clothes/ [accessed 1 July 2020].

[288] Article 5(1)(e) GDPR.

[289] Article 6d(3)(a) Wet publieke gezondheid.

[290] 'Tijdelijke Wet Notificatieapplicatie COVID-19: Memorie van Toelichting', p. 11.

[291] Article 3(2) Danish executive order.

[292] Article 5 Danish Executive order.

[293] Cite.

[294] Article II(1) Tijdelijke Wet.

[295] Article II(3) Tijdelijke Wet.

[296] Article II(4) Tijdelijke Wet.

[297] 'Tijdelijke Wet Notificatieapplicatie COVID-19: Memorie van Toelichting', p. 18.

[298] 'Tijdelijke Wet Notificatieapplicatie COVID-19: Memorie van Toelichting', p. 18.

continued. The EDPB also recommends including legal provisions on when a contact tracing app should be dismantled, and which entity is responsible for determining that.[299]

3.3.5 Interoperability

The effectiveness of contact tracing apps depends on their interoperability with other local, regional, or national contact tracing apps.[300] For example, England, Wales, Scotland, and Northern Ireland all have different contact tracing apps, though people travel frequently between those countries. On an EU level, the interoperability of contact tracing apps also supports the freedom of movement within the internal market and enables borders to remain open, facilitating travel for work and tourism.

The eHealth Network specified three key requirements for interoperability in the Common EU Toolbox: 1) the epidemiological criteria/heuristics defining close contacts for high risk exposure should be aligned, including the definition of close contact (distance and duration of exposure) as well as the period for which contacts are stored; 2) contact tracing apps should be able to register a user's proximity contacts with other users operating different contact tracing apps, and; 3) national authorities should exchange data on infection transmission chains by means of backend solutions.[301]

The eHealth Network developed these key requirements in greater detail in interoperability guidelines for contact tracing apps,[302] as well as in recommendations for basic[303] and detailed interoperability elements.[304] To enable backend server interoperability, those Member States participating in the eHealth Network developed a single federation gateway with the support of the Commission. Each national backend server for a contact tracing app can upload the keys of newly infected citizens and download the keys from other countries participating in the federation gateway.[305]

The Commission consequently issued a Decision on the functioning of the federation gateway and the modalities for the cross-border exchange of data between national authorities.[306] The Decision appoints the national authorities or official bodies processing personal data in the federation gateway (often the national public health authority or service) as joint controllers,[307] and the Commission itself as the processor of personal data processed within the federation gateway.[308]

Participation in the eHealth Network and the federation gateway is voluntary for Member States. Nonetheless, certain Member States provide for by law that their national contact tracing app should be interoperable. For instance, Belgian contact tracing app legislation states that the app should provide interoperability.[309]

[299] EDPB, 'Guidelines 04/2020', para. 31.

[300] 'Commission Recommendation (EU) 2020/518 on a common Union toolbox', para. 14.

[301] eHealth Network, 'Common EU toolbox', pp. 16–17.

[302] eHealth Network, 'Interoperability guidelines for approved contact tracing mobile applications in the EU', 2020, https://ec.europa.eu/health/sites/health/files/ehealth/docs/contacttracing_mobileapps_guidelines_en.pdf.

[303] eHealth Network, 'Basic interoperability elements between COVID+ Keys driven solutions (v1.0)', 2020, https://ec.europa.eu/health/sites/health/files/ehealth/docs/mobileapps_interoperabilityspecs_en.pdf.

[304] eHealth Network, 'Detailed interoperability elements between COVID+ Keys driven solutions (v1.0)', 2020, https://ec.europa.eu/health/sites/health/files/ehealth/docs/mobileapps_interoperabilitydetailedelements_en.pdf.

[305] eHealth Network, 'Detailed interoperability elements between COVID+ Keys driven solutions (v1.0)', p. 10.

[306] 'Commission Implementing Decision (EU) 2020/1023 of 15 July 2020 amending Implementing Decision (EU) 2019/1765 as regards the cross-border exchange of data between national contact tracing and warning mobile applications with regard to combatting the COVID-19 pandemic', https://eur-lex.europa.eu/eli/dec_impl/2020/1023/oj.

[307] Article 7a(4) 'Commission Implementing Decision (EU) 2020/1023 of 15 July 2020 amending Implementing Decision (EU) 2019/1765 as regards the cross-border exchange of data between national contact tracing and warning mobile applications with regard to combatting the COVID-19 pandemic'.

[308] Article 74(5) 'Commission Implementing Decision (EU) 2020/1023 of 15 July 2020 amending Implementing Decision (EU) 2019/1765 as regards the cross-border exchange of data between national contact tracing and warning mobile applications with regard to combatting the COVID-19 pandemic'.

[309] Article 14 § 3 (4) Koninklijk besluit.

Furthermore, each data controller on a national level should have a legal basis in national law for processing in the federation gateway.[310] Member States that participate in the federation gateway and rely on public interests for the processing of data in the context of their app may need to adjust their domestic public health law or related law to include a legal basis for the cross-border exchange of pseudonymous data originating from digital contact tracing methods.[311] Member States that rely on consent need to obtain additional consent for interoperability processing.[312] If Member States use a different legal basis than public interest or consent they may need to take other actions to ensure that the chosen legal basis covers interoperability processing via the federation gateway.

Some Member States already adopted contact tracing app legislation before they joined the federation gateway and therefore had to amend their legislation. For example, in the Netherlands the legislature adopted an amendment to the contact tracing app legislation, adding a new provision to the Public Health Act to create a legal basis for such processing.[313]

The EDPB has stressed that "[t]he goal of interoperability should not be used as an argument to extend the collection of personal data beyond what is necessary".[314] To protect against function creep after interoperability, the purpose of interoperability should be clearly specified. For example, Dutch contact tracing app legislation makes interoperability conditional on the fact that it "contributes to the goal of the early detection of possible infection from the virus by keeping track of users who have been in close proximity and alerting them about possible infection".[315] There are also other mechanisms available for Member States to exchange (aggregated and anonymized) health data, such as the Early Warning and Response System (EWRS). The sharing of pseudonymized contact tracing app data should not be merged with more general cross-border health data sharing schemes.

The ideal of interoperability creates pressure on Member States to use the Google and Apple API. The APIs released by Apple and Google enable interoperability of contact tracing apps between Android and iOS devices using apps from public health authorities.[316] This technical affordance of the GAEN further consolidates the power of these tech giants in the contact tracing app ecosystem.

3.3.6 The relationship to big tech

A topic that so far as received surprisingly little regulatory attention concerns the role of private tech companies in the deployment of digital COVID-19 solutions. With the Exposure Notification framework, two of the Big Nine joined forces to "help governments and health agencies reduce the spread of the virus, with user privacy and security central to the design."[317] In using the Google-Apple Exposure Notification Framework, governments readily outsourced yet another of their public core tasks to Big Tech, for understandable reasons, but thereby further deepening the dependency on what are essentially very large commercial operators. At the same time, governments and health agencies have no rights to transparency or control regarding the code and the protocols on the side of the platforms.[318]

[310] Recital 10 'Commission Implementing Decision (EU) 2020/1023 of 15 July 2020 amending Implementing Decision (EU) 2019/1765 as regards the cross-border exchange of data between national contact tracing and warning mobile applications with regard to combatting the COVID-19 pandemic'.

[311] EDPB, 'Statement on the data protection impact of the interoperability of contact tracing apps', para. 12.

[312] EDPB, 'Statement on the data protection impact of the interoperability of contact tracing apps', para. 12.

[313] 'Tijdelijke wet notificatieapplicatie COVID-19: Amendement van het lid Van den Berg C.S.', 2020, https://zoek.officielebekendmakingen.nl/kst-35538-12.html.

[314] EDPB, 'Statement on the data protection impact of the interoperability of contact tracing apps', para. 5.

[315] Article 6d(9) Wet publieke gezondheid.

[316] https://www.blog.google/inside-google/company-announcements/apple-and-google-partner-COVID-19-contact-tracing-technology/

[317] https://covid19.apple.com/contacttracing

[318] Veale, 2020; Cattuto & Spina, 2020.

As we argue elsewhere, regulating the relationship with external technology platforms is important for at least three reasons: 1) The reliance on the technical infrastructure of Google and Apple creates new and potentially lasting institutional dependencies, 2) in facilitating the national contact tracing app, Google and Apple are assigned an important function in executing a task in the area of public health policy, 3) Google and Apple were working on their own contact tracing app (phase two), creating considerable legal uncertainty how this would affect national contact tracing solutions. A recently discovered privacy flaw in the Exposure Notification System and Google's initial failure to address the flaw after pointed to it by researchers illustrated rather vividly how little actual safeguards member states have to identify failures and compel the tech players to deal with identified flaws.[319]

The EDPB raised the issue of security concerns, and recommended that '[t]he use of notification services provided by OS platform providers should be carefully assessed, and should not lead to disclosing any data to third parties.'[320] The European Parliament pointed to the "essential role played by the high-tech sector in ensuring the continuity of social life, businesses and administrations", and call on the European Commission "to ensure the strategic autonomy of the EU in a post-pandemic context" and the need of "investing in digital capacities, infrastructure and technologies" as a key element of national and European recovery policies.[321] On a member state level, the Dutch Advisory Committee warned the Dutch Government about the limited influence the government has over Google and Apple and suggested to bundle forces within Europe and formulate legal responses to the Google-Apple Exposure Notification Framework on a European basis.[322] In addition, the Dutch Data Protection Authority made clear that without concrete agreements with Google and Apple the app could not be launched lawfully.[323]

In the Netherlands, the Dutch Privacy Authority required contractual agreements that Google and Apple would refrain from processing personal data, the termination of the Exposure Notification Framework once the ministry decided to unable the app and the deletion of data collected, the use of phase 2 of the Notification Framework (i.e. the development and launch of an alternative contact tracing app by Google and Apple), and the proper distirbution of tasks and responsibilities vis-a-vis the processing of presonal data.[324] In a similar vein, the Italian Data Protection Authority required clarification of the relationship to platforms.

So far, only Austria, Belgium, Switzerland and Italy adopted formal regulations that prohibited third parties (like platforms) from access data gathered via the app, and only the Austrian law required that the data that is being collected was stored in Europe, and not in a public cloud. If there are agreements between national governments, Google and Apple they are, to the knowledge of the authors not public (see also: need for democratic oversight).

The most extensive regulation can be found in Switzerland. The relevant Swiss law included an obligation to enable external auditing and for this purpose access rights, the existence of contractual obligations to respect certain provisions in Swiss law and the authority of the Swiss regulatory authority to monitor compliance.[325]

[319] https://themarkup.org/privacy/2021/04/27/google-promised-its-contact-tracing-app-was-completely-private-but-it-wasnt

[320] EDPB, 'Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak' 21 April 2020, p. 16.

[321] European Parliament, 'Digital sovereignty for Europe', EPRS Ideas Paper, 2020.

[322] Raad van State, 'Tijdelijke wet notificatieapplicatie covid-19', 2020.

[323] AP, 'Advies op voorafgaande raadpleging COVID19 notificatie-app', 2020

[324] AP, 'Advies op voorafgaande raadpleging COVID19 notificatie-app', 2020, p. 17.

[325] Verordnung über das Proximity-Tracing-System für das Coronavirus Sars-CoV-2, 24 Juni 2020, Art. 10

3.4 Conclusion

The technological and regulatory approaches that have been developed, often hastily, during the current crisis will likely form an important framework for future public health emergencies. The way in which we restrict and govern new large scale data processing capabilities for public bodies such as national health agencies and Ministries of Health during the COVID-19 crisis is therefore even more important.

Contact tracing apps risk interfering with a set of fundamental rights, including the rights to privacy and data protection, the freedom of assembly and the freedom of movement. To ensure these interferences are provided for by law, contact tracing apps need to operate from a solid legal basis. In general, the GDPR's provision on consent cannot function as a sufficient legal basis for contact tracing apps. Member States therefore need to base their contact tracing apps on the grounds of public interest, which requires a clear legal basis in sector-specific law, such as a domestic public health act.

In addition to the creation of a legal basis, a regulatory framework for contact tracing apps needs to ensure the voluntary nature of the app, include several safeguards against abuse of the app and its data, oblige transparency regarding the app's operation and its source code, formulate a clear sunset clause for legislation, and legislate the interoperability of the app within the federation gateway. As Cattuto and Spina argue, "the institutionalisation of digital tools for public health also requires an institutionalisation of the regulatory framework for the design and deployment of these tools."[326] This paper has provided a first catalogue of aspects that should be covered by such a new regulatory framework.

[326] Cattuto and Spina, 'The institutionalisation of digital public health', sec. V.

4 Comparative analysis[327]

4.1 Germany in times of Corona

Germany was also among the first Western countries to be hit by the COVID-19 pandemic. On 22 March, with more than 18,000 reportedly infected and a daily peak of almost 2,000 new cases, Chancellor Angela Merkel's Cabinet issued a nation-wide ban on (public) assemblies of more than two people, along with a social-distancing obligation in public spaces of 1.5 meters.[328] Shortly after, the elected German Senate ("Bundestag") declared "an epidemiological situation of national scale", for which it approved a series of amendments to the *Infektionsschutzgesetz*,[329] bestowing the National Health Ministry with exceptional powers to autonomously adopt protective measures from the "Bundesrat".[330] Simultaneously, all 16 Federal States implemented parallel restrictions in conformity with the government's strategy.[331] Two months later, by means of a second amendment to the *Infektionsschutzgesetz*, COVID-19 and the Corona virus SARS-CoV-2 entered the list of mandatory notifiable infections.[332]

Accompanying the first restrictions, the government announced a nation-wide hackathon inspired by Estonia named "WirVSVirus", which was held over two days in March, and which sought to achieve digital solutions with public cooperation during the pandemic.[333] With over 28,000 participants and 1,500 pitches, the government claimed WirVsVirus to be the largest hackathon in the world.[334]

4.1.1 The road to the *CoronaWarn* App

As the first restrictions were implemented, the Federal Health Minister envisaged the introduction of digital contact tracing solutions as a necessary exit strategy.[335] Under the government's commission, a joint team of scientists from the Robert Koch Institute ("RKI"), the government's health agency, and other prominent research institutes began working together on the launch of an app within the PEPP-PT framework in late March.[336] However, in an unanticipated move, the government reversed its decision a few weeks later, opting for the development of an app under the Exposure Notification System introduced by Apple and Google.[337] According to the Federal State Secretary, the deviation from the original plans was primarily dictated by the need to build user trust in the app, which decentralised solutions could

[327] The research for this section was concluded in December 2020.

[328] Robert Koch Institut, 'Täglicher Lagebericht des RKI zur Corona virus-Krankheit-2019 (COVID-19)', (RKI.de, 22 March 2020) <https://www.rki.de/DE/Content/InfAZ/N/Neuartiges_Corona virus/Situationsberichte/2020-03-22-de.pdf?__blob=publicationFile> accessed 10 April 2021; Bundesministerium des Innern, für Bau und Heimat, 'Bundeskanzlerin Merkel zu den neuesten Beschlüssen von Bund und Ländern' (BMI.Bund.de, 22 March 2020) < https://www.bmi.bund.de/SharedDocs/videos/DE/pressestatements/2020/03/merkel-statement-leitlinien-Corona.html> accessed 10 April 2021.

[329] Gesetz zur Verhütung und Bekämpfung von Infektionskrankheiten beim Menschen, v. 20/07.2000 BGB1. I S. 1045.

[330] Deutscher Bundestag, 'Ja zu Gesetzen zum Bevölkerungs- und Sozialschutz und zu Krankenhäusern' (Bundestag.de, 25 March 2020) < https://www.bundestag.de/dokumente/textarchiv/2020/kw13-de-Corona-infektionsschutz-688952> accessed 10 April 2020; Gesetz zum Schutz der Bevölkerung bei einer epidemischen Lage von nationaler Tragweite, v. 27 March 2020 BGB1 S.14.

[331] Die Bundesregierung, 'Besprechung der Bundeskanzlerin mit den Regierungschefinnen und Regierungschefs der Länder vom 22.03.2020' (bundesregierung.de, 22 March 2020) < https://www.bundesregierung.de/breg-de/themen/Corona virus/besprechung-der-bundeskanzlerin-mit-den-regierungschefinnen-und-regierungschefs-der-laender-vom-22-03-2020-1733248> accessed 10 April 2021.

[332] Zweites Gesetz zum Schutz der Bevölkerung bei einer epidemischen Lage von nationaler Tragweite, v 19.05.2020 BGB1. I S. 1018, Art. 18.

[333] WirVSVirus, 'Solution Enabler' (Wirvsvirus.org, March 2020) <https://wirvsvirus.org/solution-enabler/> accessed 10 April 2021.

[334] WirVSVirus, 'Hackathon' (Wirvsvirus.org, March 2020) <https://wirvsvirus.org/hackaton/> accessed 10 April 2021.

[335] CDU, 'Jens Spahn: Es ist noch die Ruhe vor dem Sturm' (CDU.de, 26 March 2020) <https://archiv.cdu.de/artikel/jens-spahn-es-ist-noch-die-ruhe-vor-dem-sturm> accessed 10 April 2021.

[336] Die Bundesregierung, 'Regierungspressekonferenz vom 06. April 2020' (bundesregierung.de, 6 April 2020) <https://www.bundesregierung.de/breg-de/suche/regierungspressekonferenz-vom-06-april-2020-1739648> accessed 10 April 2021.

[337] Bundesministerium für Gesundheit, 'Erklärung von Kanzleramtsminister Helge Braun und Bundesgesundheitsminister Jens Spahn zur Tracing-App' (bundesgesundheitsministerium.de, 26 April 2020) <https://www.bundesgesundheitsministerium.de/presse/pressemitteilungen/2020/2-quartal/tracing-app.html> accessed 10 April 2021.

foster more suitably.[338] Moreover, he emphasised that the app would need to operate properly on mobile devices, hinting that Apple's refusal to open its interface to PEPP-PT apps may have partly influenced the change of route.[339] While MPs and activists rallied against it,[340] the new decision represented an outright contradiction of the government's position a few days prior, which highlighted concerns for the level of trust assigned to tech firms in a decentralised system when compared to the "high reliability" of a central server managed by health authorities under the PEPP-PT framework.[341]

The government eventually commissioned the development of the new *CoronaWarn* App from two leading German IT companies, Deutsche Telekom and SAP,[342] which presented the project publicly one month later.[343] On 15 June, fifty days after being announced by the Commission, *CoronaWarn* became available via Apple and Google Play stores for users nationwide, reaching 6 million downloads in only two days.[344]

4.1.2 The debate over the need for legislation for the *CoronaWarn App*

While *CoronaWarn* launched in June, debates around the need for digital contact tracing were sparked much earlier during the pandemic. In March, the Federal Health Minister included (in the aforementioned first package of reforms to the *Infektionsschutzgesetz)* a clause compelling telecommunication providers to share people's mobile data at the request of the authorities for the purpose of contact tracing.[345] The proposal triggered fierce criticism across several parliamentary factions and the offices of the federal and state data protection authorities for delivering a "blank check for surveillance" to the government and a "disproportionate attack on the fundamental rights" of citizens, and was immediately dropped.[346] However, this did not discourage the Federal Health Minister from subsequently reiterating the importance of digital contact tracing as a necessary element in Germany's pandemic exit,[347] further arguing that this would prove "much easier" than the traditional methods used by health workers.[348]

In parallel, plans for the development of a mobile app began taking shape, with the Commission to the RKI and affiliate institutes, of which the Federal Minister of Justice and the Federal Commissioner for Data Protection and Freedom of Information expressed positive opinions, under the condition the app offered sufficient guarantees for data protection and voluntary use.[349] Several State Data Protection Officers also

[338] Die Bundesregierung, 'Regierungspressekonferenz vom 27 April 2020' (bundesregierung.de, 27 April 2020) <https://www.bundesregierung.de/breg-de/suche/regierungspressekonferenz-vom-27-april-2020-1747774> accessed 10 April 2021.

[339] Ibid; Douglas Busvine and Andreas Rinke, 'Germany at odds with Apple on smartphone Corona virus contact tracing' (Reuters.com, 23 April 2020) <https://www.reuters.com/article/us-health-Corona virus-europe-tech-idUSKCN2251MR> accessed 10 April 2021; BR24 Redaktion, 'Corona-App: Bundesregierung doch für dezentrale Datnspeicherung' (Br.de, 26 April 2020) <https://www.br.de/nachrichten/deutschland-welt/Corona-app-bundesregierung-doch-fuer-dezentrale-datenspeicherung,RxEl42Q> accessed 10 April 2021.

[340] BR24, 'Netzaktivisten, SPD und Grüne begrüßen dezentrale Corona-App' (Br.de, 26 April 2020) <https://www.br.de/nachrichten/meldung/netzaktivisten-spd-und-gruene-begruessen-dezentrale-Corona-app,3002be511> accessed 10 April 2021.

[341] Die Bundesregierung, 'Regierungspressekonferenz vom 24. April 2020' (bundesregierung.de, 24 April 2020) <https://www.bundesregierung.de/breg-de/suche/regierungspressekonferenz-vom-24-april-2020-1746948> accessed 10 April 2021.

[342] Marcel Rosenbach and Hilmar Schmundt, 'Telekom und SAP sollen Entwicklung uebernehmen' (Spiegel.de, 28 April 2020) <https://www.spiegel.de/netzwelt/apps/Corona virus-t-systems-und-sap-sollen-tracing-app-entwicklung-uebernehmen-a-2c17c96e-ba53-42ba-ace4-42cd2c3215b0> accessed 4 June 2021.

[343] T-Mobile and SAP, 'Vorstellung der CoronaWarn App' (Coronawarn.app, 29 May 2020) <https://www.Coronawarn.app/assets/documents/20200529_Vorstellung-CWA.pdf> accessed 10 April 2021.

[344] Deutsche Telekom, 'In Knapp 50 Tagen programmiert: Telekom und SAP veröffentlichen Corona-Warn-App' (Telekom.com, 10 April 2021) <https://www.telekom.com/de/medien/medieninformationen/detail/telekom-sap-Corona-warn-app-in-50-tagen-programmiert-602162> accessed 10 April 2021.

[345] Entwurf zur Änderung des Infektionsschutzgesetzes und weiterer Gesetze, v. 20 March 2020 <https://fragdenstaat.de/dokumente/4075-anderung-des-infektionsschutzgesetzes-und-weiterer-gesetze>.

[346] Alexandra Föderl-Schmid, 'Wie Überwachung gegen das Virus helfen könnte' (Süddeutsche.de, 23 March 2020) <https://www.sueddeutsche.de/digital/Corona virus-smartphone-daten-tracking-ueberwachung-datenschutz-1.4855065> accessed 10 April 2021.

[347] *See above,* CDU (2020).

[348] Süddeutsche Zeitung, 'Spahn: Konsequente Suche nach Corona-Kontakterpersonen' (Sueddeutsche.de, 31 March 2020) <https://www.sueddeutsche.de/gesundheit/gesundheit-duesseldorf-spahn-konsequente-suche-nach-Corona-kontakterpersonen-dpa.urn-newsml-dpa-com-20090101-200331-99-539230> accessed 10 April 2021.

[349] Sven Böll, 'Es gibt keine Alternative zu einer freiwilligen Nutzung' (WirtschaftsWoche, 31 March 2020) <https://www.wiwo.de/my/politik/deutschland/datenschutzbeauftragter-ueber-Corona-apps-es-gibt-keine-alternative-zu-einer-freiwilligen-nutzung/25697972.html> accessed 10 April 2021; Tagesschau, "Spahn zu Lockerung des Kontaktverbots" (Tagesschau.de, 26 March 2020) <https://www.tagesschau.de/thema/Corona virus/> accessed 10 April 2021.

expressed similar concerns.[350] In the Bundestag, members of the opposition demanded the government introduce the app through a transparent process, under open source and on a voluntary basis.[351] The signatories of the motion referred specifically to voluntariness as a key-factor in gaining people's trust in technology, upon which the success or failure of the operation would ultimately depend.[352] Berlin-based Chaos Computer Club, the largest hacker association in Europe, also entered the debate with a checklist of necessary conditions for the evaluation of the app, pinning voluntariness and non-discrimination from its (non) use as pivotal requirements.[353] While there seemed to be certain public consensus on the importance of preserving voluntariness, a few politicians from the *Großkoalition* still expressed themselves in favour of mandatory download and activation, or, at least granting certain tax incentives for app users.[354]

Throughout April, the debate on voluntariness slowly grew entangled with questions of democratic legitimacy. At a press conference soon after the announcement of a first PEPP-PT app, the government's spokesperson dodged a question on the Cabinet's plans for a new regulatory scheme for the app, stating that the decision would be contingent on technical outcomes, though the app would conform to European and national standards of data protection.[355] In the midst of public criticism targeting the choice of the centralised PEPP-PT system,[356] a team of academic experts from *Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung* issued a DPIA for the decentralised models in which it deemed user consent, pursuant Art. 6 (1) GDPR, insufficient as a legal basis for voluntary use of the app, and called for the legislature to consider alternative regulatory routes.[357] At that time, fewer than 50 days before the official launch of the app and with the new commission already assigned to Telekom and SAP, the German government still expressed strong uncertainty around the political and legal process to be followed.[358]

As of May, such discussions shifted to more institutional formats, when members of the opposition parties, *Freie Demokraten* ("FDP") and *Die Grünen*, began shedding doubts on the government's strategy in the Bundestag. FDP members, in particular, called for a reinvigoration of Parliament's role in the early stages of the government's decision-making process when interfering with fundamental rights, with reference to the development of the contact tracing app.[359] The parliamentary group additionally suggested the establishment of an independent "Expert Committee for Freedoms", to supervise the process.[360] At the same time, the Grüne representatives urged Merkel's Cabinet to promptly present a separate bill for

[350] Der Landesbeauftratgte für den Datenschutz und die Informationsfreiheit Rheniland-Pfalz, 'Kann und darf das Handy gegen Corona helfen?' (datenschutz.rlp.de, 31 March 2020) <https://www.datenschutz.rlp.de/de/aktuelles/detail/news/detail/News/kann-und-darf-das-handy-gegen-Corona-helfen/> accessed 10 April 2021; Berlin.de, 'Datenschutzbeautragte sieht Handy-Ortung kritisch' (Berlin.de, 30 March 2020) <https://www.berlin.de/aktuelles/brandenburg/6125660-5173360-datenschutzbeauftragte-sieht-handyortung.html> accessed 10 April 2021.

[351] Deutscher Bundestag, 'Klare und transparente Kriterien für eine differenzierte Öffnungsstrategie', (2020) Drucksache 19/18711, 4 <https://dipbt.bundestag.de/dip21/btd/19/187/1918711.pdf> accessed 10 April 2021.

[352] ibid.

[353] Chaos Computer Club, '10 Prüfsteine für die Beurteilung von "Contact Tracing"- Apps' (ccc.de, 6 April 2020) <https://www.ccc.de/de/updates/2020/contact-tracing-requirements> accessed 10 April 2021.

[354] Jürgen Klöckner and others, 'Koalition streitet über Pflicht zur Corona-App-Nutzung' (Handelsblatt.com, 10 April 2020) <https://www.handelsblatt.com/politik/deutschland/eindaemmung-der-pandemie-koalition-streitet-ueber-pflicht-zur-Corona-app-nutzung/25731978.html?share=twitter&ticket=ST-98087-d0Pqjt1mxWIJyRzBy0Fm-ap6> accessed 10 April 2021; Redaktionsnetzwerk Deutschland, 'Corona-App: JU-Chef will automatische Installation auf allen Handys' (rnd.de, 12 April 2020) <https://www.rnd.de/politik/Corona-app-ju-chef-will-automatische-installation-auf-allen-handys-CBDOAFONE3RDKIWPNJXS53EWIQ.html> accessed 10 April 2021; Kreiszeitung, 'Stopp-Corona-App soll endlich kommen – zwei Tech-Giganten erhalten Zuschlag' (kreiszeitung.de, 16 June 2020) <https://www.kreiszeitung.de/deutschland/stopp-Corona-app-tracing-telekom-sap-datenschutz-kritik-COVID-19-zr-13644040.html> accessed 10 April 2021.

[355] Die Bundesregierung, 'Regierungspressekonferenz vom 1 April 2020' (Bundesregierung.de, 1 April 2020) <https://www.bundesregierung.de/breg-de/suche/regierungspressekonferenz-vom-1-april-2020-1738574> accessed 10 April 2021.

[356] D64 and others, 'Offener Brief: Geplante Corona-App ist höchst problematisch' (ccc.de, 24 April 2020) < https://www.ccc.de/system/uploads/299/original/Offener_Brief_Corona_App_Bundeskanzleramt.pdf> accessed 10 April 2021; Dali Kaafar and others, 'Joint Statement on Contact Tracing' (19 April 2020) <https://drive.google.com/file/d/1OQg2dxPu-x-RZzETlpV3lFa259Nrpk1J/view> accessed 10 April 2021.

[357] Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung, 'Datenschutz-Folgenabschätzung für die Corona-App' (fiff.de, 29 April 2020), 53-57 <https://www.fiff.de/dsfa-corona-file/> accessed 10 April 2021.

[358] Die Bundesregierung, 'Regierungspressekonferenz vom 4. Mai 2020' (bundesregierung.de, 4 May 2020) <https://www.bundesregierung.de/breg-de/suche/regierungspressekonferenz-vom-4-mai-2020-1750288> accessed 10 April 2021.

[359] Deutscher Bundestag, 'Rechtsstaat in der Corona-Krise verteidigen – Bürger und Freiheitsrechte bewahren', (2020) Drucksache 19/19009, 3-5 <https://dip21.bundestag.de/dip21/btd/19/190/1919009.pdf> accessed 10 April 2021.

[360] ibid.

the regulation of the app in order to boost citizens' trust, attaching detailed demands in relation to its content.[361] The law would be necessary to ensure that the app's use remained voluntary, a word that the MPs interpreted broadly to encompass a prohibition on preferential or discriminatory treatment of app (non) users and on the use of collected data for the enforcement of sanctions against violations of the restrictions, along with other data protection guarantees.[362] Outside political circles, civil society groups became particularly engaged in the discussion, siding with the opposition's claims. Digital rights activists from *Digitale Gesellschaft* demanded in an open letter to the Bundestag that MPs take the matter into their own hands by initiating an ordinary legislative procedure, whereas a group of academics went even as far as drafting a proposal for a new law to govern the app.[363] On the other hand, the FPD withdrew its original support for the initiative, prioritising the rapid availability of an open-source app.[364]

Against the government's persistant refusal of the necessity of creating a separate legal basis,[365] political pressure from the opposition escalated at the announcement of the *CoronaWarn App* in mid-June. First, it was the turn of *Die Grünen*, which presented a draft bill introducing a set of civil, labour and administrative law guarantees for the voluntariness and the purpose limitation of digital applications for contact tracing.[366] Representatives from *Die Linke* confronted the Federal Minister for Special Affairs on the matter, questioning the government's choice to avoid the legislative route notwithstanding the additional safeguards this would have offered for the voluntary use of the app, a criterion repeatedly championed by the government, and against indirect coercion emanating from social pressure.[367] The Cabinet's dismissal of the initiatives was based on the argument that such legislative demands do not arise merely because the app was not deployed as a mandatory "governmental project", but rather as an available option for download. The Cabinet also argued the current legal framework would be capable of addressing the corresponding situation in the "analogue world", in which a person could be informed by a friend who tested positively that s/he may have been infected due to recent physical interaction.[368] With respect to the opposition's concerns for horizontal discriminatory practices, the Federal Minister of Special Affairs instead argued that, while also undesirable for the government itself, it would be unrealistic for employers or businesses to enforce it, considering that use and (de-)activation of the *CoronaWarn App* would ultimately be placed under the control of the individual within its technical architecture.[369] Notably, the Federal Ministry of Justice's official advisor for consumer issues did not share the latter position, arguing that a law would have instead strengthened the initiative's legitimacy.[370]

[361] Deutscher Bundestag, 'Demokratie, Bürgerrechte und Zivilgesellschaft in Zeiten der Corona-Krise' (2020) Drucksache 19/18958, 4 <https://dip21.bundestag.de/dip21/btd/19/189/1918958.pdf> accessed 10 April 2021.

[362] ibid.

[363] Digitale Gesellschaft, 'Offener Brief: Bundestag müss über Corona-App entscheiden' (digitalegesellschaft.de, 7 May 2020) < https://digitalegesellschaft.de/2020/05/offener-brief-bundestag-muss-ueber-corona-app-entscheiden/> accessed 10 April 2021; Malte Engeler and others, 'Vorschlag für ein Gesetz zur Einführung und zum Beitrieb einer App-basierten Nachverfolgung von Infektionsrisiken mit dem SARS-CoV-2 (Corona) Virus', (2020) Version 1.0 <https://www.malteengeler.de/wp-content/uploads/2020/05/Vorschlag-fu%CC%88r-ein-Gesetz-zur-Einfu%CC%88hrung-und-zum-Betrieb-einer-App-basierten-Nachverfolgung-von-Infektionsrisiken-mit-dem-Corona-Virus-Version-1.0.pdf> accessed 10 April 2021.

[364] IT-Zoom, 'Grüne beharren auf Gesetz für Corona-Warn-App' (IT-ZOOM, 4 June 2020) https://www.it-zoom.de/mobile-business/e/gruene-beharren-auf-gesetz-fuer-Corona-warn-app-26002/ accessed 10 April 2021.

[365] Zeit Online, 'Bundesjustizministerin halt Extra-Gesetz für Corona-App für unnotig' (zeit.de, 15 June 2020) <https://www.zeit.de/politik/deutschland/2020-06/Corona-app-christine-lambrecht-pflicht-gesetz-bundesjustizministerin-datenschutz> accessed 10 April 2021.

[366] Deutscher Bundestag, 'Entwurf eines Gesetzes zur zivil-, arbeits- und dienstrechtlichen Sicherung der Freiwilligkeit der Nutzung und nur Zweckbindung mobile elektronischer Anwendungen zur Nachverfolgung von Infektionsrisiken', (2020) Drucksache 19/20037 <https://dipbt.bundestag.de/doc/btd/19/200/1920037.pdf> accessed 10 April 2021.

[367] Deutscher Bundestag 165. Sitzung, 17 June 2020, Plenarprotokoll 19/165, 20534 <http://dipbt.bundestag.de/doc/btp/19/19165.pdf#P.20522> accessed 10 April 2021.

[368] Ibid, 20534.

[369] Ibid.

[370] Sachverständigenrat für Verbraucherfragen, 'Regierungsberater fordern Gesetz für Corona-Warn-App' (svr-verbraucherfragen.de, 15 June 2020) <https://www.svr-verbraucherfragen.de/presse/pressespiegel/> accessed 11 April 2021.

Meanwhile, the RKI issued a DPIA for the launched app, in which it supported the government's view that consent would constitute an appropriate legal basis.[371] The Federal Commissioner for Data Protection and Freedom of Information, and several of his counterparts across the German States also did not make any objections in this regard.[372] However, the controversy would not die out until the last parliamentary hearings in the summer. When asked by members of *Alternative für Deutschland*, why the government had refused to create a law for the *CoronaWarn App*, the latter replied that the existing data protection rules would suffice to prevent the much feared discrimination or marginalisation of non-users.[373] The reason provided was that employers and businesses conducting controls over the app's installation on others' mobile phones would under said circumstances assume the position of a data controller with no valid legal ground, considering that the consent given by a user when downloading the app would be insufficient to this end.[374]

At present, no law has come into being for the app.

4.1.3 Recent developments around the *CoronaWarn App*

Almost six months since its deployment, the *CoronaWarn App* has reached almost 23 million downloads, of which 6 million were already reached by the second day.[375] While the app was praised in its initial months of operation,[376] confidence in the app has recently diminished, in light of the critiques advanced by prominent politicians,[377] scientists, [378]and the Federal Minister of Health himself, who however reassured the public that this would not affect the voluntary nature of the app.[379]

4.2 Italy in times of Corona

4.2.1 Italy and the initial phase of the pandemic

Italy was the first and most seriously hit Western country during the initial outbreak of the COVID-19 pandemic in February and March 2020. In order to face the rapid increase in infection and mortality rates, and the risks associated with the region's inadequate healthcare infrastructure, the government implemented a full lockdown on 9 March that would last until the beginning of May. Alongside applying restrictions on physical movement, Premier Giuseppe Conte's Cabinet pursued a strategic action plan to proactively counteract the spreading of the virus, starting with the appointment of an *ad hoc*

[371] Robert Koch Institut, 'Corona Warn-App:Bericht zur Datenschutz-Folgenabschätzung für die Corona-Warn-App der Bundesrepublik Deutschland', (2021) Version 1.7, 64-67 <HYPERLINK „https://www.coronawarn.app/assets/documents/cwa-datenschutz-folgenabschaetzung.pdf"https://www.coronawarn.app/assets/documents/cwa-datenschutz-folgenabschaetzung.pdf > accessed 11 April 2021.

[372] BfDI, 'Sufficient data protection in the Corona warning app' (bfdi.bund.de, 16 June 2020) <https://www.bfdi.bund.de/EN/Home/Press_Release/2020/12_Corona-Warning-App.html> accessed 11 April 2021; Gesellschaft für Datenschutz und Datensicherheit, 'Corona-Warn-App- Expertenbeiträge und Ansichten der Aufsichtsbehörden' (gdd.de, 16 June 2020) <https://www.gdd.de/datenschutz-und-Corona/Datenspende%20Apps%20und%20Corona%20Tracing> accessed 11 April 2021.

[373] Deutscher Bundestag, 'Antwort der Bundesregierung', (2020) Drucksache 19/21197, 3 <https://dip21.bundestag.de/dip21/btd/19/211/1921197.pdf>

[374] ibid.

[375] Robert Koch Institut, 'Kennzahlen zur Corona-Warn-App' (rki.de, 19 November 2020) <https://www.rki.de/DE/Content/InfAZ/N/Neuartiges_Corona virus/WarnApp/Archiv_Kennzahlen/Kennzahlen_20112020.pdf?__blob=publicationFile> accessed 11 April 2021; *See above* Deutscher Bundestag (2020), 20523.

[376] Bundesministerium für Gesundheit, 'Spahn: Die App ist ein Werkzeug von vielen, um neue Ausbrüche einzudämmen'

[377] Manuel Höferlin, 'Bundesregierung muss Corona-Warn-App endlich nachbessern' (fdpbt.de, 20 November 2020) <https://www.fdpbt.de/hoeferlin-bundesregierung-muss-Corona-warn-app-endlich-nachbessern> accessed 11 April 2021; BR24 Redaktion, 'Söder: Corona-Warn-App "Bisher ein zahnloser Tiger"' (Br.de, 20 October 2020) <https://www.br.de/nachrichten/deutschland-welt/ministerpraesident-markus-soeder-corona-warn-app-bisher-ein-zahnloser-tiger,SDvt9w1> accessed 11 April 2021.

[378] Lisa Fröhlich, 'Sinn und Unsinn der Corona-Warn-App' (TraceCorona.net, 13 October 2020) <https://traceCorona.net/de/2020/10/13/sinn-und-unsinn-der-corona-warn-app/> accessed 11 April 2021; Zeit Online, 'Ärzteverband hält Corona-App für wenig hilfreich' (zeit.de, 24 September 2020) <https://www.zeit.de/digital/mobil/2020-09/corona-app-aerzteverband-infektionsschutz-wirksamkeit-gesundheitsamt> accessed 11 April 2021.

[379] Ärzte Zeitung, 'Spahn: Mehr Menschen sollten Infektionen über Corona-App melden' (aerztezeitung.de, 8 November 2020) <https://www.aerztezeitung.de/Politik/Spahn-Mehr-Menschen-sollten-Infektionen-ueber-Corona-App-melden-414463.html> accessed 11 April 2021.

Extraordinary Commissioner vested with special powers to manage the health crisis.[380] In the following days, the government announced it would also explore various technological solutions to contain the pandemic, based on the "South Korean model". A public call for contributions was therefore launched on 24 March, inviting companies, institutions and organisations to submit proposals for the development of digital solutions in the field of telemedicine and the home care of patients, as well as for the active monitoring of infection risks.[381] The Italian Health Ministry received more than 300 submissions for the latter.

4.2.2 The road to *Immuni*

The government established an interdisciplinary task force by means of executive decree shortly after the conclusion of the consultation to conduct a socio-economic and epidemiological study of governmental containment measures, with particular focus on the impact of data driven technologies.[382] The 74 experts were divided into eight working subgroups (WSG), among which WSG 6 ("On Technologies for crisis management") was tasked with the technical and impact assessment of the proposals submitted in response to the public call.[383] A complementary judicial and normative analysis of such data-driven solutions was assigned to WSG 8 ("On legal perspectives around data processing related to the emergency").[384] The majority of recommendations included in the WSG's final reports revolved around the development of a digital system for contact tracing, in the form of a mobile app.[385] The evaluative process of the proposed technological solutions, consisting of three distinct phases, culminated with the selection of two candidate applications, namely *COVIDApp* and *Immuni.*[386] The public procurement was eventually awarded to *Immuni*, developed by Milan-based *Bending Spoons S.p.a,* in light of its suitability for promptly combatting the virus, its compatibility with the European PEPP-PT model, and the guarantees it offered for privacy protection, as explained in the Extraordinary Commissioner's decree 10/2020 formalising the decision.[387] After the government obtained a free license from its developers to operate the app, *Immuni* was made available for download on 1 June for both Google and Apple operating systems.[388]

4.2.3 The debate on the need for legislation for *Immuni*

Right from the start of the government's digital strategy for the containment of the pandemic, public debate around the introduction of a mobile contact tracing app raised the issue of its democratic legitimacy In a series of interviews with major national news outlets, the Italian Data Protection Authority (DPA) welcomed the measure, only if it was implemented in an adequate and proportionate manner for the fulfilment of its objectives.[389] In particular, the DPA highlighted the importance of developing a legal framework to ensure that the deployment of contact tracing tools conformed to those principles for the duration of the national state of emergency.[390] The Health Minister's scientific advisor also confirmed

[380] Decreto-Legge 17 Marzo 2020, n.18, Art. 122 < https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legge:2020-03-17;18!vig=~art122> accessed 11 April 2021.

[381] MITD, 'Telemedicina e sistemi di monitoraggio, una call per tecnologie per il contrasto al COVID-19' (innovazione.gov.it, 23 March 2020) <https://innovazione.gov.it/notizie/articoli/telemedicina-e-sistemi-di-monitoraggio-una-call-per-tecnologie-per-il-contrasto-a/> accessed 11 April 2021.

[382] Presidenza del Consiglio dei Ministri, 'Gruppo di Lavoro COVID 19', (March 2020), Art. 2 <https://assets.innovazione.gov.it/1612352551-dm-gruppo-di-lavoro-COVID-19-signed.pdf> accessed 11 April 2021

[383] ibid, Art. 2.2-3

[384] ibid.

[385] Fidelia Cascini and others, 'Impiego di tecnologie di digital contact tracing' in Servizio Studi del Senato, *Tracciamento di Contatti: Elementi di documentazione* (2020), 49 <https://www.senato.it/service/PDF/PDFServer/BGT/01151447.pdf> accessed 11 April 2021; Sottogruppo di lavoro "Profili giuridici della gestione dei dati connessa all'emergenza", 'Relazione tecnico-giuridica sui profile connessi all'eventuale adozione di una soluzione di contact tracing per il contrasto al COVID-19' (2020) <https://raw.githubusercontent.com/taskforce-covid-19/documenti/master/sgdl_8_Profili_Giuridici_Gestione_Dati_Emergenza/sgdl8_relazione_profili_giuridici_contact_tracing.pdf> accessed 11 April 2021.

[386] Ibid.

[387] Il Commissario Stroardinario, 'Ordinanza n. 10/2020', (April 2020), 2 <http://www.governo.it/sites/new.governo.it/files/CSCOVID19_Ord_10-2020_txt.pdf> accessed 11 April 2021.

[388] Immuni, 'Let's start afresh together' (immuni.italia.it, 1 June 2020) <https://www.immuni.italia.it/> accessed 11 April 2021.

[389] Garante per la Protezione dei Dati Personali, 'Soro, la sfida privacy in era Corona virus. Garante, sì misure straordinarie, ma proporzionate e tempranee' (garanteprivacy.it, 17 March 2020) <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9292565> accessed 11 April 2021.

[390] Garante per la Protezione dei Dati Personali, 'Soro: Sì al tracciamento dei contatti ma con un decreto temporaneo' (garanteprivacy.it, 26 March 2020) <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9299193> accessed 11 April 2021.

that before the app's launch, privacy concerns should be addressed with the drafting of an *ad hoc* legal instrument.[391]

Political tensions began escalating in reaction to the Extraordinary Commissioner's decree, which awarded the procurement for a national app to *Bending Spoons S.p.a.* for *Immuni.*[392] Members of right-wing opposition parties specifically contested the procedure that led to the selection of the app, demanding the Parliament's immediate involvement. In their opinion, the decision could not possibly be adopted in "*Huxleyan*" style by the mere decree of an interim executive official.[393] In its address to the Italian Senate shortly after the publication of the Extraordinary Commissioner's decree, the Prime Minister reassured the public that *Immuni* would be made available only on a voluntary basis, albeit omitting any mention of the Cabinet's plan to subject the regulation of the app to the democratic process.[394] The Prime Minister merely assured the public that the government would commit to allowing for democratic oversight on the operation of the app, by keeping the Parliament regularly updated on its implementation.[395] However, several MPs still complained about a lack of clarity *ab initio* on the identity of data processors and controller, the location of the app's server, and the nature of the required consent from Italian citizens.[396] The arguments brought forward from the opposition benches were also shared by prominent members of the ruling parties, who insisted on the necessity of a legal instrument to safeguard the fundamental freedoms at stake from personal data mismanagement and discriminatory outcomes for *Immuni* users.[397]

A few weeks later, Conte eventually signed "Decreto Legge 30 Aprile 2020, n. 28" (*Decreto Legge*) outlining general criteria for the development of *Immuni*. These included the requirement of voluntariness for the download of the app,[398] the choice of the Minister of Health as data controller,[399] a prohibition on the use of geolocation data,[400] an obligation to treat collected data anonymously or, when impossible, pseudonymously.[401] The *Decreto Legge* also guaranteed no discriminatory repercussions on the lives of citizens for failing to download the app.[402] The decision would later be cheered by members of the governing coalition for bringing transparency and clarity to the use of the *Immuni* app.[403] However, the Parliament still exposed points of criticism.

After the conclusion of a series of private hearings with members of the Cabinet, the Parliamentary Security Committee regarded the law as delineating a rather broad framework which still deferred important decisions on the criteria for data processing to the responsible ministers.[404] In the Committee's view, the law also failed to specify the legal status of alerts received through the app and the consequences for incompliant behaviour.[405] Despite acknowledging the value of the anti-discrimination clause enshrined in

[391] Federico Giuliani, 'Già pronto il modello coreano. Parte l'assalto al Corona virus' (IlGiornale.it, 21 March 2020) <https://www.ilgiornale.it/news/mondo/Corona virus-lultima-idea-dellitalia-imitare-modello-1844050.html> accessed 11 April 2021.

[392] *See above,* Il Commissario Straordinario (2020), 2.

[393] Camera dei Deputati, Seduta n. 329, 22 April 2020 <http://banchedati.camera.it/tiap_18/ctrStartPage.asp> accessed 11 April 2021.

[394] Senato della Repubblica, 208a Seduta pubblica, 21 April 2020 <http://www.senato.it/3818?seduta_assemblea=9101> accessed 11 April 2021.

[395] ibid.

[396] Open Redazione, 'Corona virus, l'app Immuni slitta? Per ora mette d'accordo Pd, Forza Italia e Lega: Serve una legge sui dati personali' (open.online, 20 April 2020) <https://www.open.online/2020/04/20/Corona virus-app-immuni-slitta/> accessed 11 April 2021.

[397] Deputati PD, 'Corona virus. Delrio. Per uso app tracciamento serve legge' (deputatipd.it, 20 April 2020) <https://deputatipd.it/news/%E2%80%8B%E2%80%8B%E2%80%8B%E2%80%8B%E2%80%8BCorona virus-delrio-uso-app-tracciamento-serve-legge> accessed 11 April 2021.

[398] Decreto Legge 30 Aprile 2020, n. 28, GU Serie Generale n. 111, Art 6.1 <https://www.gazzettaufficiale.it/eli/id/2020/06/29/20A03469/sg> accessed 11 April 2021.

[399] Ibid.

[400] Ibid, Art. 6.2c.

[401] ibid, Art. 6.2d.

[402] ibid, Art. 6.4.

[403] Camera dei Deputati, Seduta n. 361, 24 Giugno 2020 <https://www.camera.it/leg18/410?idSeduta=0361&tipo=stenografico> accessed 11 April 2021.

[404] Comitato Parlamentare per la Sicurezza della Repubblica, 'Relazione sui profile di sicurezza del Sistema di allerta COVID-19 previsto dall'articolo 6 del decreto-legge n.28 del 30 Aprile 2020' (2020), 12 <https://documenti.camera.it/_dati/leg18/lavori/documentiparlamentari/IndiceETesti/034/002/intero.pdf> accessed 11 April 2021.

[405] Ibid.

Art. 6.4, the Committee found its text to be insufficient for the prevention of horizontal restrictions based on the installation and use of the app, thereby prejudicing the requirement of voluntariness under Art. 6.1.[406]

The opposition therefore advanced several amendments aimed at increasing privacy safeguards through the introduction of criminal sanctions for violations and illegitimate sharing of citizens' data collected via the app,[407] and of more explicit responsibilities for the Ministry of Health to ensure that the operation of the app be suspended pursuant to the deadline prescribed by law.[408] Another motion instead demanded the establishment of a three-month buffer period, during which the government, consulting with the DPA, could identify critical issues of privacy and security and accordingly suspend the operation of *Immuni* with all related data processing.[409] The ruling coalition, however, did not incorporate amendments, holding that the original text of the law already guaranteed and ensured all necessary safeguards, notwithstanding the desirability of further privacy protection.[410]

In addition to the content of the law, the opposition was also critical of the procedural route chosen by the government. The aforementioned *Decreto Legge* is an Italian legislative device which may be signed into law by the Prime Minister in extraordinary circumstances independently from Parliament, provided that it is presented to the parliamentary chambers on the same day of its announcement and is converted into a law within 60 days.[411] Conte's repeated efforts to resort to special executive powers since the pandemic's outbreak and regulate the freedom of movement and economic policy has perplexed MPs and scholars, raising serious doubts about the constitutionality of some of the measures.[412] Whereas the *Decreto Legge* would still offer an opportunity for democratic scrutiny *ex post*, it also needs to be pointed out that Art. 6 of the *Decreto Legge* framing the use of the app was hastily inserted into a chaotic regulatory package, addressing a wide spectrum of issues of criminal law and procedure which bore no connection to digital contact tracing.[413] According to some MPs, given the sensitivity and long-term impact of many of such themes, they should have instead been addressed within the context of more fundamental organic reforms, for which the legislature should have invested more time and resources. This is contrary to the pressing circumstances imposed by the adoption of a *Decreto Legge* and especially by the vote of confidence attached by the government to the success of its conversion into law later in June.[414] Notwithstanding the DPA's approval of the *Decreto Legge* as the relevant legal framework,[415] discussions in Parliament also highlighted the inconsistency of the government's decision to launch the public call and select the app before drafting an actual law with Parliament that would have made the role of technology in the state of the emergency clear, as well as understanding its social and economic impact, and gaining the trust of citizens.[416]

[406] ibid, 13.

[407] Camera dei Deputati, 'Ordine del Giorno in Assemblea su P.D.L. 9/02547/008', 24 June 2020 <https://aic.camera.it/aic/scheda.html?numero=9/2547/8&ramo=C&leg=18> accessed 11 April 2021.

[408] Camera dei Deputati, 'Ordine del Giorno in Assemblea su P.D.L. 9/02547/010' 24 June 2020 <https://aic.camera.it/aic/scheda.html?numero=9/2547/10&ramo=C&leg=18> accessed 11 April 2021.

[409] Camera dei Deputati, 'Ordine del Giorno in Assemblea su P.D.L. 9/02547/026 <https://aic.camera.it/aic/scheda.html?numero=9/2547/26&ramo=C&leg=18> accessed 11 April 2021.

[410] Camera dei Deputati, Seduta n. 362, 25 June 2020 <http://banchedati.camera.it/tiap_18/ctrStartPage.asp> accessed 11 April 2021.

[411] Costituzione della Repubblica Italiana, Art. 77.

[412] *See* Francesco S Marini, 'Le deroghe costituzionali da parte dei decreti-legge', *Federalismi.it*, (2020) <https://www.federalismi.it/ApplOpenFilePDF.cfm?artid=42106&dpath=document&dfile=22042020160817.pdf&content=Le%2Bderoghe%2Bcostituzionali%2Bda%2Bparte%2Bdei%2Bdecreti%2Dlegge%2B%2D%2Bstato%2B%2D%2Bpaper%2B%2D%2B>; *See* Giovanni Ruggiero, 'Fase 2, Renzi bombarda Conte: <<Calpesta la Costituzione: ora basta, la libertà non vale meno della salute>>' (open.online, 28 April 2020) <https://www.open.online/2020/04/28/fase-2-renzi-bombarda-conte-calpesta-costituzione-liberta-vale-piu-salute/> accessed 11 April 2021.

[413] *See above,* Decreto Legge 30 April 2020, Art. 1-5.

[414] Camera dei Deputati, Seduta n. 361, 24 June 2020 <https://www.camera.it/leg18/410?idSeduta=0361&tipo=stenografico> accessed 11 April 2021; *See* Camera dei Deputati, 'Decreto giustizia, posta la questione di fiducia' (camera.it, 23 June 2020) <https://www.camera.it/leg18/1132?shadow_primapagina=10764> accessed 11 April 2021.

[415] Garante per la Protezione dei Dati Personali, 'Parere sulla Proposta normative per la previsione di una applicazione volta al tracciamento dei contagi da COVID-19', doc. Web.n. 9328050, 29 April 2020, <https://www.camera.it/leg18/1132?shadow_primapagina=10764> accessed 11 April 2021.

[416] Camera dei Deputati, Seduta n. 333, 30 April 2020 <https://www.camera.it/leg18/410?idSeduta=0333&tipo=stenografico> accessed 11 April 2021.

The opposition also contested the opacity of the decision-making process on the basis of which *Immuni* was chosen over other applicants.[417] As illustrated above, the special task force set up by the government to conduct a techno-judicial analysis of the proposals submitted during public consultation concluded its report by recommending both *Immuni* and *COVIDApp* as the two final candidates to be tested. There seemed to be some confusion as to what happened afterwards. Although in an official communication to Conte, the Minister of Innovation and Digitalisation ("MID") reported that the task force found *Immuni* the most suitable solution, however no such conclusion could be reached from the latter's analysis.[418] The MID subsequently retracted the statement, declaring before the Parliamentary Security Committee that the choice of *Immuni* had been ultimately motivated by the advanced state of the project, which would have allowed the government to deploy the app within a shorter timeframe.[419] In the same hearing before the Committee, the MID also revealed that the Director of the Italian National Intelligence Services ("DIS") had provided a technical opinion to Ministers during the selection process, whereas several journalistic inquiries discovered that his involvement may have been more central than what the MID claimed to be as mere advice.[420] By then, two weeks had already passed since the publication of the aforementioned Extraordinary Commissioner's decree officially adopting the app.

Moreover, the process also seemed to have been affected by the inconsistent application of the criteria designed for the selection of the apps, which *Immuni* did not exhaustively fulfil at that time.[421] According to the MID, the determining factor for her preference over *COVIDApp* amounted to *Immuni*'s higher predisposition for development under PEPP-PT,[422] as formally confirmed by the Extraordinary Commissioner in his decree.[423] However, with Apple and Google releasing their exposure notification framework,[424] the MID suddenly averted from her original plan and announced the app would follow the tech giants' decentralised framework, instead of the originally envisaged PEPP-PT.[425] In light of this, the MID's earlier claims regarding the task force's "selection" of the app appeared weaker, considering the weight assigned to the PEPP-PT in the original decision.

4.2.4 *Immuni* and more recent developments

The *Decreto Legge* would eventually be voted upon in Parliament and passed into law devoid of amendments on 25 June 2020,[426] though *Immuni* had already been launched the same month. Today, the app's official website counts more than 10 million downloads and 73,000 notifications sent by users.[427] *Immuni*'s limited success prompted the government to react publicly, given the surging infection rate after the summer of 2020. The Prime Minister's initial appeal to the people's "moral obligation" to download and use the app soon transformed into a temptation to render it mandatory for access to certain

[417] Ibid.

[418] Il Ministro per l'Innovazione Tecnologica e la Digitalizzazine, 'COVID-19: audizione informale Ministro Pisano in 8a Commissione', 29 April 2020 <https://assets.innovazione.gov.it/1609773866-relazioneaudizione2904viiicommissionesenato.pdf> accessed 11 April 2021; Luciano Capone, 'L'App anti virus scelta con una manipolazione del Ministro Pisano' (ilfoglio.it, 5 May 2020) <https://www.ilfoglio.it/tecnologia/2020/05/05/news/lapp-anti-virus-scelta-con-una-manipolazione-del-ministro-pisano-316639/> accessed 11 April 2021.

[419] *See above,* Comitato Parlamentare per la Sicurezza della Repubblica (2020), 10.

[420] Ibid; Lidia Baratta and Nicola Biondo, 'Ma quindi chi ha scelto (e che fine ha fatto) la app Immuni?' (linkiesta.it, 7 May 2020) <https://www.linkiesta.it/2020/05/scelta-app-immuni-bending-spoons-trasparenza/> accessed 11 April 2021; Paola Pisano, 'La fake su Immuni. Replica del ministro Pisano (e risposta)' (ilfoglio.it, 7 May 2020) <https://www.ilfoglio.it/politica/2020/05/07/news/le-fake-su-immuni-replica-del-ministro-pisano-e-risposta-316993/> accessed 11 April 2021.

[421] IRPA, 'Luci e ombre sulla procedura di selezione di "Immuni", l'app del governo di tracciamento del contagio da COVID-19' (Irpa.eu, May 2020) <https://www.irpa.eu/luci-e-ombre-sulla-procedura-di-selezione-di-immuni-lapp-del-governo-di-tracciamento-del-contagio-da-COVID-19/> accessed 11 April 2021.

[422] *See above,* Ministero dell'Innovazione e della Digitalizzazione, 3.

[423] *See above,* Il Commissario Straordinario (2020), 2.

[424] Apple, 'Apple and Google partner on COVID-19 contact tracing technology' (apple.com, 10 April 2020) <https://www.apple.com/newsroom/2020/04/apple-and-google-partner-on-COVID-19-contact-tracing-technology/> accessed 11 April 2021.

[425] Ministro per l'Innovazione tecnologica e la transizione digitale, 'Le domande sulla App Immuni della trasmissione Report' (innovazione.gov.it, 11 May 2020) <https://innovazione.gov.it/notizie/comunicati-stampa/le-domande-sulla-app-immuni-della-trasmissione-report/> accessed 11 April 2021.

[426] Legge 25 Giugno 2020, n. 70, GU Serie Generale n. 162 del 29-06-2020.

[427] Immuni, 'The numbers of Immuni' (immuni.italia.it, 11 April 2021) <https://www.immuni.italia.it/dashboard.html> accessed 11 April 2021.

public spaces.[428] The idea, however, remained confined to private Cabinet discussions and as also assured by the DPA, never materialised.[429]

4.3 The UK in times of Corona

The rate of COVID-19 infections increased relatively late in the UK[430] in comparison to other European countries.[431] Departing from its milder approach in the first weeks of the crisis,[432] Her Majesty's Government announced on 23 March the temporary closure of hospitality and entertainment businesses, as well as recommendations to the public to stay home and avoid social contact as much as possible.[433] Due to the limited capacities of the country's health authorities to deal with the overwhelming number of cases, the British Cabinet put a halt to traditional contact tracing, but then resumed it the following month.[434]

In cooperation with other research institutes, the National Health Service ("NHS") launched a public hackathon for the development of data-driven solutions to limit the spread of the virus.[435] Although the event represented a major step for the implementation of digital technologies in the fight against the pandemic, it did not reach the same participation rate and media attention as its European counterparts. Prime Minister Boris Johnson also outlined a strategy to reverse the tide of the virus within three months, making prominent reference to the use of "new digital technology" for tracing the disease.[436]

4.3.1 The road to the *NHS app*

The plans for a contact tracing app for the UK officially emerged in a press conference given by the Health and Social Care Secretary ("the Health Secretary"), who presented the initiative as a side-measure to the strengthening of manual tracing methods.[437] As assignee of the project, the NHSX, the NHS arm responsible for digital transformation, publicly communicated its intentions to pursue the development of a centralised system for the app under the supervision of an *ad hoc* ethical board.[438] Despite pressures from privacy experts to switch to a decentralised version,[439] the NHSX decided to maintain its original preference, while working with Apple to ensure it would avoid technical constraints imposed by the tech company's API.[440] On 4 May, the Health Secretary revealed the app would be deployed for pilot testing on

[428] Il Fatto Quotidiano, 'Immuni, l'appello di Conte:"Scaricarla è un obbligo morale verso gli altri". Da metà ottobre dialogherà con le altre app europee" (ilfattoquotidiano.it, 2 October 2020) <https://www.ilfattoquotidiano.it/2020/10/02/immuni-lappello-di-conte-scaricarla-e-un-obbligo-morale-verso-gli-altri-da-meta-ottobre-dialoghera-con-le-altre-app-europee/5952458/> accessed 11 April 2021.

[429] Presidente del Garante per la Protezione dei Dati Personali, 'Memoria del Presidente del Garante per la protezione dei dati personali sul ddl di conversion in legge del decreto-legge 7 Ottrobre 2020, n.125, recante misure urgenti connesse con la proroga della dichiarazione dello stato di emergenza epidemiologica da COVID-19 e per la continuità operativa del Sistema di allerta COVID, nonché per l'attuazione della direttiva (UE) 2020/739 del 3 GIugno 2020' (Privacy.it, 19 October 2020) <https://www.privacy.it/2020/10/21/garante-proroga-emergenza-COVID/> accessed 11 April 2021.

[430] We refer in this report to only England and Wales under the term "UK", considering that Scotland and Northern Ireland opted for separate digital contact tracing strategies.

[431] UK Government, 'People tested positive' (Corona virus.data.gov.uk, 25 March 2020) <https://Corona virus.data.gov.uk/details/cases> accessed 26 April 2021.

[432] UK Government, 'Prime Minister's statement on Corona virus (COVID-19)' (gov.uk, 12 March 2020) <https://www.gov.uk/government/speeches/pm-statement-on-corona virus-12-march-2020> accessed 26 April 2021.

[433] UK Government, 'Government announces further measures on social distancing' (gov.uk, 20 March 2020) <https://www.gov.uk/government/news/government-announces-further-measures-on-social-distancing> accessed 26 April 2021.

[434] Sarah Boseley, 'UK to start Corona virus contact tracing again' (The Guardian, 17 April 2020) <https://www.theguardian.com/world/2020/apr/17/uk-to-start-Corona virus-contact-tracing-again> accessed 26 April 2021.

[435] OdiLeeds, 'Open Data Saves Lives' (odileeds.org, 26 March 2020) <https://odileeds.org/projects/open-data-saves-lives/COVID19/> accessed 26 April 2021.

[436] UK Government, 'Prime Minister's statement on Corona virus' (gov.uk, 20 March 2020) <https://www.gov.uk/government/speeches/pm-statement-on-corona virus-20-march-2020> accessed 26 April 2021.

[437] UK Government, 'Health and Social Care Secretary's statement on Corona virus' (gov.uk, 12 April 2020) <https://www.gov.uk/government/speeches/health-and-social-care-secretarys-statement-on-corona virus-COVID-19-12-april-2020> accessed 26 April 2021.

[438] NHSX, 'Digital Contact Tracing: Protecting the NHS and Saving Lives' (nhsx.nhs.uk, 24 April 2020) <https://www.nhsx.nhs.uk/blogs/digital-contact-tracing-protecting-nhs-and-saving-lives/> accessed 26 April 2021.

[439] Martin Albrecht and others, 'Joint Statement' (29 April 2020) <https://drive.google.com/file/d/1uB4LcQHMVP-oLzIIHA9SjKj1uMd3erGu/view> accessed 26 April 2021.

[440] *See above,* NHSX (2020).

the Isle of Wight[441] amid concerns from MPs and experts over alleged persistent technical difficulties.[442] Although the app was originally intended to launch 28 May, the government postponed its roll-out a few weeks,[443] and later re-routed the app under Apple-Google's decentralised framework due to experiencing technical failures, delaying it again until 24 September.[444] In a hearing before Parliament, the Health Secretary, and later the NHSX, explained that it was the tech companies' intervention that determined their change of plans, and consequent delays and waste of financial resources.[445]

4.3.2 The debate on the need for legislation for the *NHS app*

The process spanning the conception and the implementation of the *NHS app* was remarkably characterised by a series of unilateral and, at times, opaque decisions by the UK government, in which the Parliament only marginally had a say.

From the outset, the Health Secretary's plan for digital contact tracing promised to put citizens' privacy at its core, conforming to the highest ethical and security standards, and in particular, the principles of data minimisation, transparency and proportionality.[446] Notwithstanding a leaked document exposing the NSHX's original temptation to allow the de-anonymisation of users' data,[447] the commitment to ensure sufficient data protection seemed to remain a central pillar of the Cabinet's strategy.[448]

These reassurances did not, however, suffice to put a halt to MPs' concerns. Since the announcements of the first centralised and the second decentralised model respectively in April and June, doubts from the opposition about the necessity of a legislative basis for the processing of the app's data began circulating within the House of Commons and the House of Lords.[449] Speakers from the government dismissed the claims with vague references to the voluntary nature of the app.[450]

The peak of the debate was however reached with a series of inquiries of the Joint Committee on Human Rights ("the Committee"), which, before the disclosure of the plans for the app, had already played an active role scrutinising the government's exit strategy.[451] In a letter to the Health Secretary on 28 April, the Committee insisted on obtaining certain governmental guarantees for the implementation of review and oversight mechanisms to ensure that a voluntary and privacy-friendly app could be deployed.[452] The letter moreover contained an explicit request to the Cabinet for the introduction of specific legislation regulating the use of digital technologies during the pandemic, and to be wary of discriminatory outcomes for (digitally) disadvantaged categories.[453]

[441] UK Government, 'Health and Social Care Secretary's statement on Corona virus (COVID-19)' (gov.uk, 4 May 2020) <https://www.gov.uk/government/speeches/health-and-social-care-secretarys-statement-on-Corona virus-COVID-19-4-may-2020> accessed 26 April 2021.

[442] HC Deb 17 June 2020, vol 677, col 820; Leo Kelin, 'Corona virus: UK contact-tracing app is ready for isle of Wight downloads' (bbc.com, 4 May 2020) <https://www.bbc.com/news/technology-52532435> accessed 26 April 2021.

[443] UK Government, 'Government launches NHS Test and Trace service' (gov.uk, 27 May 2020) <https://www.gov.uk/government/news/government-launches-nhs-test-and-trace-service> accessed 26 April 2021.

[444] UK Government, 'Health and Sociale Care Secretary's statement on Corona virus (COVID-19)' (gov.uk, 18 June 2020) <https://www.gov.uk/government/speeches/health-and-social-care-secretarys-statement-on-Corona virus-COVID-19-18-june-2020> accessed 26 April 2021.

[445] Ibid; UK Parliament, 'Plans for digitally transforming the NHS' (Parliament.uk, 6 November 2020) <https://publications.Parliament.uk/pa/cm5801/cmselect/cmpubacc/680/68006.htm> accessed 26 April 2021.

[446] *See above,* UK Government (12 April 2020).

[447] David Pegg and Paul Lewis, 'NHS Corona virus app: memo discussed giving ministers power to 'de-anonymise' users' (The Guardian, 13 April 2020) <https://www.theguardian.com/world/2020/apr/13/nhs-Corona virus-app-memo-discussed-giving-ministers-power-to-de-anonymise-users> accessed 26 April 2021.

[448] *See above,* NHSX (2020).

[449] HC Deb 28 April 2020, vol 675, col 199; HL Deb 19 May 2020, vol 803, col 1084; HL Deb 25 June 2020, vol 804, col 604.

[450] Ibid.

[451] Letter from Harriet Harman MP to Matt Hancock (9 April 2020) <https://committees.parliament.uk/publications/650/documents/2721/default/> accessed 26 April 2021.

[452] Letter from Harriet Harman to Matt Hancock (28 April 2020) <https://committees.parliament.uk/publications/819/documents/5290/default/> accessed 26 April 2020.

[453] Ibid.

The Health Secretary's reply showed certain awareness of the potential impact of the contact tracing technology on vulnerable groups, highlighting the efforts of the government to include advocacy groups in relevant discussions.[454] On the other hand, the Health Secretary outrightly rejected the proposal for an *ad hoc* legal framework for the app, claiming the initiative fell within the Health Department's autonomous competences prescribed in times of national crisis.[455] Thus, the Health Secretary voiced the view that the GDPR and the Human Rights Act were sufficient in providing the necessary legal safeguards.[456] Meanwhile, the Committee issued a report evaluating the government's past and envisaged steps in this regard.[457] Its recommendations were also sent as a letter to the Health Department, in which the Chair of the Committee reiterated the importance of putting the guarantees illustrated by the Health Secretary into formal legislation, considering that the "mishmash" of intersecting legal regimes might be inadequate in protecting people's interests.[458] On this point, the report stressed that the general public could experience difficulties in understanding the applicable rules without an *ad hoc* law for digital contact tracing.[459] Secondly, the MPs also demanded that a Special Human Rights Commissioner be appointed and given oversight and enforcement powers to guard against abuses of rights beyond privacy and data protection, which would not fall within the mandate of the already existing Information Commissioner's Office ("ICO").[460] To this end, the Committee's Chair attached a draft bill to the letter, confident that it would be promptly passed by Parliament to roll-out the *NHS App.*[461] The proposed law took into account several of the previously exposed concerns, ranging from transparency duties for the authorities[462] to common data protection safeguards, such as voluntary consent, limits to data retention, purpose specification, and periodical reviews for the necessity of contact tracing measures.[463] The law also provided for monetary sanctions against anyone, other than the authorised entities or by decree of the Secretary of State, processing or collecting digital contact tracing data.[464] A group of academic experts consulted by Parliament produced a similar draft, though placing more emphasis on direct and indirect anti-discrimination safeguards against potential coercive use of the app.[465]

The arguments, however, were not sufficiently convincing. Although the ICO agreed that a broader domain of rights could be at stake, for example in labour or anti-discrimination law, it found that the applicable data protection regime could suitably address demands of fairness, proportionality and transparency due to its "strong flexibility".[466] The Health Secretary rejected the proposal, restating the government's commitments to transparency and security within the framework of the Data Protection Act 1998 and Human Rights Act 1998.[467] Despite the Committee's further insistence in delivering a comparative overview of the relevant protection loopholes under present legislation against the new bill, the government made no concessions.[468]

[454] Letter from Matt Hancock to Harriet Harman (4 May 2020) <https://publications.parliament.uk/pa/jt5801/jtselect/jtrights/correspondence/200504-Response-from-Matt-Hancock-MP-regarding-Governments-plan-to-use-digital-technologies.pdf> accessed 26 April 2021.

[455] Ibid.

[456] ibid.

[457] Joint Committee on Human Rights, *Human Rights and the Government's Response to COVID-19: Digital Contact Tracing* (third report) <https://publications.parliament.uk/pa/jt5801/jtselect/jtrights/343/343.pdf> accessed 26 April 2021.

[458] Letter from Harriet Harman to Matt Hancock (7 May 2020) <https://publications.Parliament.uk/pa/jt5801/jtselect/jtrights/correspondence/Letter-to-Rt-Hon-Matt-Hancock-MP-Secretary-of-State-for-HSC-Draft-Bill.pdf> accessed 26 April 2021.

[459] *See above,* Joint Committee on Human Rights (2020).

[460] Joint Committee on Human Rights, *The Government's response to COVID-19: human rights implications,* Oral Evidence, 4 May 2020) <https://committees.Parliament.uk/oralevidence/334/pdf/> accessed 26 April 2021.

[461] *See above*, Harriet Harman (7 May 2020).

[462] Ibid, s 14.

[463] Ibid, s 11-13.

[464] Ibid, s 9.

[465] Lilian Edwards and others, 'The Corona virus (Safeguards) Bill 2020: Proposed protections for digital interventions and in relation to immunity certificates' (LawArXiv, 6 May 2020) <https://osf.io/preprints/lawarxiv/yc6xu/> accessed 26 April 2021.

[466] *See above*, Joint Committee on Human Rights (4 May 2020), q 20.

[467] Letter from Matt Hancock to Harriet Harman (21 May 2020) <https://committees.Parliament.uk/publications/1223/documents/10345/default/> accessed 26 April 2021.

[468] Letter from Harriet Harman to Matt Hancock (29 May 2020) <https://committees.Parliament.uk/publications/1284/documents/11453/default/> accessed 26 April 2021.

At the start of the initial tests on the Isle of Wight, the ICO remarked on the need for a DPIA prior to the app's launch, but not for a supplementary legal basis, admitting that consent could be sufficient for the processing of contact tracing data.[469] The NSHX issued a first DPIA reporting no particular privacy-related risks, and subsequently requested the ICO to informally review it as an independent party.[470] An academic enquiry illustrated several pitfalls within the NHSX document, including the lack of a specified lawful basis for the app's denial of access to delete it and other constraints to privacy protection inherent in its centralised design.[471] It is also relevant to note that some MPs within the Committee contested the ICO's partisan role in the process, due to its involvement in the design phase, upon which they had based their demands for the immediate establishment by law of a supervisory commissioner for contact tracing.[472] The ICO rejected the allegations.[473]

With the sudden retreat from the centralised framework in June and the government's change of priorities with respect to digital contact tracing,[474] the Parliament eventually welcomed the decision to adopt the decentralised model developed by Apple and Google.[475] This did not, however, suppress the echoing demands for a new legislative instrument to prevent digital exclusion and horizontal discrimination even up to the last days before the app's release, also in light of the many "high-profile missteps" previously committed and likely to endanger citizens' privacy if repeated.[476] Nevertheless, the NHSX still stood by the government's position when adopting the relevant legal bases for contact tracing data processing, namely a combination of both the fulfilment of its legal obligations under existing national law and user consent.[477] The government's new and recently updated DPIA did not reflect such concerns.[478]

4.3.3 Recent developments

On September 24, 2020, the *NHS COVID-19 App* was launched in England and Wales, after further tests on the Isle of Wight and Newham.[479] The government reported 6 million downloads within the first 24 hours, reaching almost 20 million in November.[480] Currently, the government is also considering the idea of introducing financial support for citizens receiving an alert notification to stay at home through the app, an option which should become available with the release of the next updated version.[481]

[469] ICO, 'COVID19 Contact Tracing: data protection expectations on app development' (ico.org.uk, 2020), 6 <https://ico.org.uk/media/for-organisations/documents/2617676/ico-contact-tracing-recommendations.pdf> accessed 26 April 2021.

[470] NHSX, ; ICO, 'Statement in response to media enquiries about the Data Protection Impact Assessment for the NHSX's trial of contact tracing app' (ico.org.uk, 7 May 2020) < https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/05/dpia-for-the-nhsx-s-trial-of-contact-tracing-app/> accessed 26 April 2021.

[471] Michael Veale, 'Analysis of the NHSX Contact Tracing App 'Isle of Wight' Data Protection impact Assessment' (LawArXiv Papers, 9 May 2020) <https://osf.io/preprints/lawarxiv/6fvgh> accessed 26 April 2021.

[472] *See above,* Joint Committee on Human Rights (2020), 12.

[473] Letter from Elizabeth Denham to Harriet Harman (11 May 2020) <https://committees.Parliament.uk/publications/1037/documents/8502/default/> accessed 26 April 2021.

[474] Sarah Boseley, 'NHS COVID-19 contact-tracing app for UK will not be ready before winter' (The Guardian, 17 June 2020) <https://www.theguardian.com/society/2020/jun/17/nhs-COVID-19-contact-tracing-app-no-longer-a-priority-says-minister> accessed 26 April 2021.

[475] Joint Committee on Human Rights, 'The Government's response to COVID-19: human rights implications' (seventh report), s 6 <https://committees.Parliament.uk/work/218/the-governments-response-to-COVID19-human-rights-implications/publications/> accessed 26 April 2021.

[476] Ibid.

[477] NHS, 'NHS App Privacy policy' (nhs.uk, 17 May 2021), v 3.8 <https://www.nhs.uk/nhs-services/online-services/nhs-app/nhs-app-legal-and-cookies/nhs-app-privacy-policy/> accessed 4 June 2021.

[478] UK Government, 'The NHS COVID-app: data protection impact assessment' (gov.uk, September 2020) <https://www.gov.uk/government/publications/nhs-COVID-19-app-privacy-information/nhs-COVID-19-app-data-protection-impact-assessment> accessed 26 April 2021.

[479] UK Government, 'NHS COVID-19 App launches across England and Wales'(gov.uk, 24 September 2020) <https://www.gov.uk/government/news/nhs-COVID-19-app-launches-across-england-and-wales> accessed 26 April 2021.

[480] Leo Kelion, 'NHS COVID-19 app to issue more self-isolate alerts' (BBC.com, 29 October 2020) <https://www.bbc.com/news/technology-54733534> accessed 26 April 2021.

[481] Rory Cellan-Jones, 'Corona virus: NHS COVID-19 app to gain self-isolation payments' (BBC.com, 30 November 2020) <https://www.bbc.com/news/technology-55133926> accessed 26 April 2021.

4.4 The Netherlands in times of Corona

An initial outbreak of the pandemic in the southern regions of the Netherlands urged the government to adopt its first anti-COVID-19 measures in mid-March. In the first phase of the crisis, the "intelligent-lockdown" approach pursued by the Dutch authorities led to milder restrictions in comparison with other European countries, placing more emphasis on each person's sense of social responsibility to manage interpersonal contacts in line with the government's health guidelines.[482] In the second phase of the pandemic, with infections rising and the resources for manual contact tracing proving inadequate, Premier Mark Rutte and his team rapidly turned to data-driven strategies for the containment of the virus. The government organised a live-streamed "appathon" for the identification of smart digital solutions against Corona one weekend in April, after the launch of a public consultation by the Minister of Public Health, Sport and Wellbeing ("the Minister"), in which a committee of experts tested and analysed seven pre-selected candidate apps.[483] The national data protection authority ("Dutch DPA"") subsequently evaluated the technical and judicial findings, which highlighted the insufficiency or lack of technical details over the presented apps, as well as the Cabinet's failure to demonstrate the necessity for such an intrusive tool.[484] NGO Bits Of Freedom also warned that no social necessity seemed to warrant the "chaotic and hasty" procedure chosen by the Cabinet for the adoption of a contact tracing app.[485] Similar concerns were shared by both Dutch and international academics.[486]

4.4.1 The road to the *CoronaMelder*

In light of the negative feedback received from authorities and civil society, the Minister of Health (the "Minister") outlined an alternative fourfold strategy before the House of Representatives ("*Tweede Kamer"),* in which he would cooperate with a new team of experts selected from the appathon for the development of a Corona app.[487] Accordingly, the new app would be developed in a transparent manner, under open source license, and within the API framework created by Google and Apple that month.[488] The *CoronaMelder* would only be publicly announced later in July, contrary to the Minister's original intention to have the app available for the summer holidays.[489] After a series of technical tests and a first positive DPIA by the Dutch DPA, the Minister declared the app ready to be launched nationally for 1 September.[490]

[482] Government of the Netherlands, 'New measures to stop spread of Corona virus in the Netherlands' (government.nl, 12 March 2020) <https://www.government.nl/topics/Corona virus-COVID-19/news/2020/03/12/new-measures-to-stop-spread-of-Corona virus-in-the-netherlands> accessed 1 May 2021.

[483] Rijksoverheid, 'Terugblik appathon' (rijksoverheid.nl, 20 April 2020) <https://www.rijksoverheid.nl/onderwerpen/Corona virus-app/tijdpad-proces-Corona virus-app/terublik-appathon> accessed 1 May 2021.

[484] Autoriteit Persoonsgegevens, 'Onderzoeksrapportage bron- en contactopsporingsapps' (autoriteitpersoonnsgegevens.nl, 20 April 2020) <https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/onderzoeksrapportage_bron-_en_contactopsporingsapps.pdf> accessed 1 May 2021.

[485] Rejo Zenger, 'Burgerrechtenorganisaties slaan alarm over werkwijze Ministerie Volksgezondheid' (bitsoffreedom.nl, 17 April 2020) <https://www.bitsoffreedom.nl/2020/04/17/burgerrechtenorganisaties-slaan-alarm-over-werkwijze-ministerie-volksgezondheid/> accessed 1 May 2021.

[486] Natali Helberger and others, 'Kijk kritisch naar nut en noodzaak Corona-apps' (uva.nl, 14 April 2020) <https://www.uva.nl/content/nieuws/nieuwsberichten/2020/04/kijk-kritisch-naar-nut-en-noodzaak-Corona-apps.html> accessed 1 May 2021.

[487] Ministerie van Volksgezondheid, Welzijn en Sport, 'Kamerbrief COVID-19: Update stand van zaken' (rijksoverheid.nl, 22 April 2020), 38 <https://www.rijksoverheid.nl/ministeries/ministerie-van-volksgezondheid-welzijn-en-sport/documenten/kamerstukken/2020/04/21/kamerbrief-COVID-19-update-stand-van-zaken> accessed 1 May 2021.

[488] Rijksoverheid, 'Kamerbrief landelijke introductie 'CoronaMelder" (rijksoverheid.nl, 16 July 2020), 20 <https://www.rijksoverheid.nl/onderwerpen/Corona virus-app/documenten/kamerstukken/2020/07/16/kamerbrief-over-landelijke-introductie-Coronamelder> accessed 1 May 2021.

[489] Rijksoverheid, 'Letterlijke tekst persconferentie minister-president Rutte en minister de Jone na afloop van crisiberaad kabinet' (rijksoverheid.nl, 3 June 2020) <https://www.rijksoverheid.nl/documenten/mediateksten/2020/06/03/letterlijke-tekst-persconferentie-minister-president-rutte-en-minister-de-jonge-na-afloop-van-crisisberaad-kabinet> accessed 1 May 2021.

[490] Rijksoverheid, 'Kamerbrief landelijke introductie "CoronaMelder"' (rijksoverheid.nl, 16 July 2020), 1-6 <https://www.rijksoverheid.nl/onderwerpen/Corona virus-app/documenten/kamerstukken/2020/07/16/kamerbrief-over-landelijke-introductie-Coronamelder> accessed 1 May 2021.

However, based on the Dutch DPA recommendation to refrain from launching the app before creating a legal basis, the Minister postponed activating the app for one month, although it was already available for download on Google and Apple stores.[491] Due to further political tensions in Parliament, the *CoronaMelder* would only become operative on 10 October.[492]

4.4.2 The debate on the need for legislation for the *CoronaMelder*

The process leading up to the introduction of a contact tracing app in the Netherlands was characterised by a continuous inter-institutional dialogue lasting several months. After the government announced its plan to develop an app, it immediately established direct communication with the *Tweede Kamer,* allowing members to follow and discuss the various steps being taken in the following months. In the first series of press conferences and official statements to MPs, the Minister and Prime Minister Rutte emphasised the importance of supporting the work of the health authorities with digital contact tracing, while repeatedly assuring the public that the Cabinet would consider the necessary privacy guarantees for citizens.[493]

In line with prominent voices from civil society and academia, some parties during the first hearings criticised the Cabinets' confidence in the necessity of a contact tracing app and its disregard for wider societal implications.[494] Similar claims would be brought forward again by the *Groenlinks* fraction at an advanced stage of the political process.[495] Although such views did not strongly resonate across the board, the initial parliamentary debates revealed a general consensus in the need to involve democratic representatives in the Cabinet's strategy.[496] The Minister therefore guaranteed the government would make no decision regarding a public procurement contract, nor create a strategy for the app's deployment without prior consultation with the *Tweede Kamer*.[497]

A turning point in the debate was reached with the appathon's failure. In its first opinion issued shortly after the event, the Dutch DPA noted that the insufficiency of technical details provided with the app submissions, the absence of a specific legal framework, and the absence of specifics on the data processing purposes obstructed the due evaluation of the relevant privacy guarantees.[498] The analysis also mirrored the findings of the State Attorney's Office, leading the government to consequently reroute its plans.[499] In an official written communication, the Minister explained that although he was impressed with the public engagement during the event, a team would need to be set up for the refinement of security, privacy,

[491] Autoriteit Persoonsgegevens, 'Advies op voorafgaande raadplegigng COVID19 notificatie-app' (autoriteitpersoonsgegevens.nl, 6 August 2020) <https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/advies_voorafgaande_raadpleging_Coronamelder-app.pdf> accessed 1 May 2021.

[492] Joost Schellevis and Nando Kasteleijn, 'CoronaMelder vandaag gelanceerd, maar 'app' is geen wondermiddel' (nos.nl, 10 October 2020) <https://nos.nl/artikel/2351727-Coronamelder-vandaag-gelanceerd-maar-app-is-geen-wondermiddel> accessed 1 May 2021.

[493] Ministerie van Volksgezondheid, Welzijn en Sport, 'COVID-19 Update stand van zaken' (rijksoverheid.nl, 7 April 2020) <https://www.rijksoverheid.nl/onderwerpen/Corona virus-app/documenten/kamerstukken/2020/04/07/kamerbrief-over-stand-van-zaken-COVID-19> accessed 1 May 2021; Rijksoverheid, 'Letterlijke tekst persconferentie na ministerraad 17 April 2020' (rijksoverheid.nl, 17 April 2020) <https://www.rijksoverheid.nl/onderwerpen/Corona virus-app/documenten/mediateksten/2020/04/17/letterlijke-tekst-persconferentie-na-ministerraad-17-april-2020> accessed 1 May 2021.

[494] Tweede Kamer der Staten Generaal, 'Ontwikkelingen rondom het Corona virus', Vergaderjaar 2019-2020, TK 67 <https://www.tweedekamer.nl/debat_en_vergadering/plenaire_vergaderingen/details/activiteit?id=2020A01494> accessed 1 May 2021; Tweede Kamer der Staten Generaal, 'Ontwikkelingen rondom het Corona virus', Vergaderjaar 2019-2020, TK 68, 11 <https://www.tweedekamer.nl/debat_en_vergadering/plenaire_vergaderingen/details/activiteit?id=2020A01617> accessed 1 May 2021; Tweede Kamer der Staten Generaal, 'Ontwikkelingen rondom het Corona virus', Vergaderjaar 2019-2020, TK 69, 40 <https://www.tweedekamer.nl/debat_en_vergadering/plenaire_vergaderingen/details/activiteit?id=2020A01692> accessed 1 May 2021.

[495] Tweede Kamer der Staten Generaal, 'Tijdelijke wet notificatieapplicatie COVID-19', vergaderjaar 2019–2020, 35 538, nr. 10, 4 <https://zoek.officielebekendmakingen.nl/kst-35538-10.pdf> accessed 1 May 2021.

[496] *See above*, Tweede Kamer der Staten Generaal (8 April 2020), 2; Motie d.d. 16 april 2020 – E. Ouwehand, Tweede Kamerlid, 'Gewijzigde motie van het lid Ouwehand over privacy experts betrekken bij de inzet van medische apps' (t.v.v. 25295-231) <https://www.tweedekamer.nl/debat_en_vergadering/plenaire_vergaderingen/details/activiteit?id=2020A01618> accessed 1 May 2021.

[497] *See above,* Tweede Kamer der Staten Generaal (16 April 2020), 41.

[498] *See above,* Autoriteit Persoonsgegevens (2020), 8.

[499] Landsadvocaat, 'Samenvatting privacy-analyse contactonderzoekapps (rijksoverheid.nl, 19 April 2020) <https://www.rijksoverheid.nl/onderwerpen/Corona virus-app/documenten/publicaties/2020/04/19/samenvatting-privacy-analyse-contactonderzoeksapps> accessed 1 May 2021.

fundamental rights and inclusion contours of the new app.[500] Next to the Dutch DPA and the State Attorney's study, the Minister also mentioned private consultancy company KPMG and the Dutch Council of Human Rights as relevant influential sources on the reversal of the government's decision.[501]

As the *CoronaMelder* was in development, discussions around the democratic legitimacy of the app bled into the broader public debate about the government using its executive powers to extend restrictive measures implemented in the initial phase of the crisis. Among other critiques, the Council of State, which advised the Cabinet on legal and governance issues, warned that such prolonging of special executive powers could result in unacceptable violations of formal parliamentary oversight and the restriction of citizens' fundamental rights.[502] The Council of State therefore declared that introducing a law for that purpose would be desirable from a democratic perspective, an idea already circulating among MPs regarding a separate legal instrument for the regulation of a contact tracing app.[503]

The Cabinet eventually drafted a law and released it for discussion at the beginning of June.[504] Interestingly, the proposed regulation contained a new legal basis for the implementation of digital contact tracing solutions, granting health authorities authorisation to process particular categories of personal data (i.e. health data), as well as discretionary powers to determine more specific rules for the management, protection and retention of said information.[505] The provision also aimed at preserving the voluntary nature of these tools by prohibiting "direct or indirect" coercion on the public to use them.[506]

Before the bill could be introduced for parliamentary scrutiny, the Council of State critiqued the text in an official recommendation to the government, recommending the removal of the relevant article, Art. 58v, from the draft.[507]

The Council of State stated that in light of the ongoing expected discussions on the political and societal implications of using such digital tools, the provision would have slowed down the legislative process to the detriment of the draft law's objective, namely that of ensuring the prompt introduction of a legal basis for the fundamental rights restrictions adopted during the pandemic.[508] Though surprised by the Council's advice, the government renounced its plans to launch the *CoronaMelder* after the summer holidays and followed suit,[509] officially declaring that it would consider drafting a separate legal basis as the relevant framework for the app.[510]

Notwithstanding the promises made to the *Tweede Kamer,* the Minister proceeded to deploy a test-version of the *CoronaMelder* in five Dutch regions on 17 August, reaching 800,000 downloads during its first day in Apple and Google stores.[511] The decision conflicted with the DPIA published by the Dutch DPA on the same day, but received a week earlier by the government,[512] in which the technical privacy

[500] *See above,* Ministerie van Volksgezondheid, Welzijn en Sport (22 April 2020), 38.

[501] Ibid.

[502] Raad van State, 'Voorlichting van grondwettelijke aspecten van (voor)genomenen crisismaatregelen', Kamerstukken II 2020/21, 25295, nr. 312 <https://www.raadvanstate.nl/@121106/w04-20-0139-vo/> accessed 2 May 2021.

[503] Ibid; Tweede Kamer der Staten-Generaal, 'Infectieziektenbestrijding' Vergaderjaar 2019-2020, 25295, n. 314, 8-34 <https://www.tweedekamer.nl/debat_en_vergadering/commissievergaderingen/details?id=2020A01700> accessed 2 May 2021.

[504] Consultatieversie van *Tijdelijke bepalingen in verband met maatregelen ter bestrijding van de epidemie van COVID-19 voor de langere termijn* (Tijdelijke wet maatregelen COVID-19) <https://www.raadsleden.nl/files/documenten/twm_COVID-19_consultatieversie.pdf> accessed 2 May 2021.

[505] Ibid, Art. 58v.1.

[506] ibid, Art. 58v.2.

[507] Raad van State, 'Tijdelijke wet maatregelen COVID-19' Kamerstukken II 2019/20, 35526, nr. 4.

[508] Ibid.

[509] *See above,* Tweede Kamer der Staten-Generaal (2020), 3.

[510] Rijksoverheid, 'Landelijke invoering Corona virus-app Coronamelder gepland op 1 September' (rijksoverheid.nl, 16 July 2020) <https://www.rijksoverheid.nl/actueel/nieuws/2020/07/16/landelijke-invoering-Corona virus-app-Coronamelder-gepland-op-1-september> accessed 2 May 2021.

[511] RTLnieuws, 'CoronaMelder al bijna 800.000 keer gedownload' (rtlnieuws.nl, 20 August 2020) <https://www.rtlnieuws.nl/tech/artikel/5178587/Coronamelder-al-bijna-800000-keer-gedownload> accessed 2 May 2021.

[512] *See above,* Tweede Kamer der Staten-Generaal (2020), 58.

guarantees offered by the app were still deemed insufficient.[513] In its assessment, the Dutch DPA observed that such safeguards would also be undermined by the inadequacy of the legal framework constructed around the data processing done through the *CoronaMelder.[514]* In the Dutch DPA's view, user consent under Art. 6 GDPR would prove insufficient to that end, and it therefore invited the government to initiate a fast-tracked legislative procedure to create *an ad* hoc law. The Dutch DPA explained that consent could effectively be relied upon only when the affected users could retain "strong" control over the processing of their personal data, which would not be the case in the context of digital contact tracing due to the constraints imposed by the app's decentralised framework.[515] A legal analysis commissioned by the Cabinet for the State Attorney instead found the Dutch DPA's conclusions unconvincing.[516] Following the advice of the Dutch DPA, the Minister promptly forwarded a fast-tracked law to the *Tweede Kamer*, which established a separate legal basis for the implementation and use of the *CoronaMelder.[517]* The Cabinet would later publish an amended version of the law,[518] following the input of *Tweede Kamer* members,[519] the Council of State,[520] and civil society.[521] While the original text aimed at ensuring the voluntary character of the *CoronaMelder* with a prohibition on direct coercion to use the app, several MPs insisted on writing a more extensive notion of voluntariness in the final draft.[522] Art. 6d(8) in fact was expanded to forbid obligations to use the app, share information and the communication of received notification therefrom, or download it to access buildings or facilities, exercise one's profession, make use of a service, engage in any form of interpersonal contact, or to receive any advantage.[523] The final text of the law also includes a detailed list of all relevant information processed by the Minister and the Municipal Health Authorities ("GGD") and the relevant data controllers in pseudonymous form.[524] Moreover, Art. II allows for the measures to be withdrawn before or extended beyond the three month period as of their entry into force, by means of executive decree.[525] The bill was generally well-received by MPs, who particularly supported the introduction of an anti-abuse clause as a central aim of the legislation, for the respect of citizens' autonomy and the prevention of social inequality.[526] It was also argued that the law would contribute to fostering trust in the app needed from the public.[527] On the other hand, some major points of criticism persisted even in this final phase

[513] Autoriteit Persoonsgegevens, 'AP: Privacy gebruikers Corona-app nog onvoldoende gewaarborgd' (autoriteitpersoonsgegevens.nl, 17 August 2020) https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-privacy-gebruikers-Corona-app-nog-onvoldoende-gewaarborgd accessed 2 May 2021; Autoriteit Persoonsgegevens, 'Advies op voorafgaande raadpleging COVID19 notificatie-app' (2020), 9 <https://www.rijksoverheid.nl/documenten/rapporten/2020/08/06/advies-op-voorafgaande-raadpleging-COVID19-notificatie-app> accessed 2 May 2021.

[514] Ibid.

[515] ibid, 11-12.

[516] Pels Rijcken, 'Juridische analyse- advise Autoriteit Persoonsgegevens inzake de DPIA van de CoronaMelder' (2020) in opract van de Minister van Volksgezondheid, Welzijn en Sport, 10 <https://www.rijksoverheid.nl/documenten/publicaties/2020/08/12/juridische-analyse-advies-autoriteit-persoonsgegevens-inzake-de-dpia-van-de-Coronamelder> accessed 2 May 2021.

[517] Tijdelijke bepalingen in verband met de inzet van een notificatieapplicatie bij de bestrijding van de epidemie van COVID-19 en waarborgen ter voorkoming van misbruik daarvan, Vergaderjaar 2019-2020, 35538, n.2 <https://zoek.officielebekendmakingen.nl/kst-35538-2.html> accessed 2 May 2021.

[518] Gewijzigd Voorstel van *Tijdelijke bepalingen in verband met de inzet van een notificatieapplicatie bij de bestrijding van de epidemie van COVID-19 en waarborgen ter voorkoming van misbruik daarvan*, Vergadeerjaar 2019-2020, 35538, n. A < https://zoek.officielebekendmakingen.nl/kst-35538-A.html> accessed 2 May 2021.

[519] Tweede Kamer der Staaten Generaal, 'Notificatieapplicatie COVID-19', Vergadeerjaar 2019-2020, TK 96-6, 15-17 <https://www.tweedekamer.nl/downloads/document?id=8e7fd992-a298-4d19-9c61-4ed030f79641&title=Notificatieapplicatie%20COVID-19.pdf > accessed 2 May 2021.

[520] Raad van State, 'Tijdelijke wet notificatieapplicatie COVID-19', Kamerstukken II 2019/2020, 35538, nr.4 <https://www.raadvanstate.nl/@121776/w13-20-0254-iii/> accessed 2 May 2021.

[521] Rejo Zenger, 'Een wet om ons tegen de bijwerkingen van een Corona-app te beschermen' (bitsoffreedom.nl, 3 September 2020) <https://www.bitsoffreedom.nl/2020/09/03/een-wet-om-ons-tegen-de-bijwerkingen-van-een-Corona-app-te-beschermen/> accessed 2 May 2021.

[522] Tweede Kamer der Staten Generaal, 'Tijdelijke wet notificatieapplicatie COVID-19' (tweedekamer.nl, 2 September 2020) <https://www.tweedekamer.nl/kamerstukken/plenaire_verslagen/kamer_in_het_kort/tijdelijke-wet-notificatieapplicatie-COVID-19> accessed 2 May 2021.

[523] Gewijzigd Voorstel van *Tijdelijke bepalingen in verband met de inzet van een notificatieapplicatie bij de bestrijding van de epidemie van COVID-19 en waarborgen ter voorkoming van misbruik daarvan*, Art. 6d (8).

[524] Ibid, Art. 6d (1) – (2).

[525] Ibid, Art. II (1) – (3).

[526] *See above,* Tweede Kamer der Staten Generaal (2020), 6 – 26.

[527] Speech of Kees van der Staaij to the Tweede Kamer der Staten Generaal, Vergaderjaar 2020-2021, 96e vergadering <https://www.tweedekamer.nl/kamerstukken/plenaire_verslagen/detail/a4993fc3-d517-423d-93ce-b6c6470fc87c> accessed 2 May 2021.

of the legislative process. Notwithstanding the Minister' s reassurance in a letter to the *Tweede Kamer*[528] that the tests on the *CoronaMelder* had detected no privacy risks, some parliamentarians still opposed the fundamental choice to deploy a contact tracing app, complaining that the letter failed to provide a democratic opportunity to decide on its necessity in view of the larger societal impact.[529] Further queries were made regarding the role of Google and Apple in processing data, and regarding the government's role in making arrangements with the tech giants for the application of their "exposure notification framework" in the country.[530]

The amended draft was eventually approved and forwarded to the Dutch Senate ("*Eerste Kamer*") for review, where the debate largely mirrored what happened in the *Tweede Kamer*.[531] The law was approved with 51 votes in favour and 19 against,[532] entering into force on 10 October 2020.

4.4.3 Recent developments around the *CoronaMelder*

The *CoronaMelder* would be activated on the same day nationally, with more than two million downloads recorded since August.[533] At present, the app's official website reports that over 4.8 million people have installed the app.[534]

4.5 Concluding observations

The Corona pandemic in Western Europe has not only highlighted systemic deficiencies in public infrastructure in addressing health crises, but also the unpreparedness of governments to provide far-sighted responses in the governance of technology in the public sector. Digital contact tracing, in particular, has triggered alarming signals for the future integrity of European democratic processes. Notwithstanding the different individual routes pursued by their respective officials, the political and legal processes in the four countries studied here share similar dynamics and fallacies, leaving room to draw general observations.

4.5.1 The need for a law

In line with the focus of this chapter, the first element of comparison lies directly with the nature of the debate on the (un)necessity of a legislative basis accompanying the apps' deployment. A distinguishing feature of these processes has certainly been the various Cabinets' confidence in the role of contact tracing technologies and especially in their undisputed necessity. While all officials showed certain willingness to discuss regulatory solutions for their use at a later stage, there seemed no room for, or even interest in, questioning the fundamental decision to invest in apps, with representatives of minor Dutch parties and academic experts constituting the sole exception. The same confidence was also displayed

[528] Ministerie van Volksgezondheid, Welzijn en Sport, 'Kamerbrief over voortgang Coronamelder' (rijksoverheid.nl, 28 August 2020) <https://www.rijksoverheid.nl/documenten/kamerstukken/2020/08/28/voortgang-Coronamelder> accessed 2 May 2021.

[529] *See above,* Tweede Kamer der Staten Generaal (2 September 2020), 81; Speech of Eva van Esch to the Tweede Kamer der Staten Generaal, Vergaderjaar 2020-2021, 96e vergadering <https://www.tweedekamer.nl/kamerstukken/plenaire_verslagen/detail/a4993fc3-d517-423d-93ce-b6c6470fc87c> accessed 2 May 2021.

[530] Motie d.d. 2 September 2020 – S van der Graaf and K Buitenweg, 'Motie over afspraken over het expure notification framework' (t.v.v. 35538-18) <https://www.tweedekamer.nl/kamerstukken/detail?id=2020Z15414&did=2020D33354> accessed 2 May 2021.

[531] Tweede Kamer der Staten Generaal, 'Stemmingen Notificatieapplicatie COVID-19', Vergadeerjaar 2020-2021, TK 97 < https://www.tweedekamer.nl/debat_en_vergadering/plenaire_vergaderingen/details/activiteit?id=2020A03535> accessed 2 May 2021; Eerste Kamer der Staten Generaal, Vergaderjaar 2020-2021, 3e vergadering < https://www.eerstekamer.nl/verslag/20201005/verslag> 2 May 2021; Eerste Kamer der Staten Generaal, Vergaderjaar 2020-2021, 4e vergadering <https://www.eerstekamer.nl/verslag/20201006/verslag> accessed 2 May 2021.

[532] Eerste Kamer der Staten Generaal, 'Eerste Kamer stemt in met Coronamelder' (eerstekamer.nl, 6 October 2020) <https://www.eerstekamer.nl/nieuws/20201006/eerste_kamer_stemt_in_met> accessed 2 May 2021.

[533] Redactie NU.nl, 'Corona-app 2,6 miljoen keer gedownload, maar hoeveel mensen gebruiken 'm?' (nu.nl, 12 October 2020) <https://www.nu.nl/tech/6083468/Corona-app-26-miljoen-keer-gedownload-maar-hoeveel-mensen-gebruiken-m.html> accessed 2 May 2021.

[534] CoronaMelder, 'Voorkom verpsreiding, download CoronaMelder' (Coronamelder.nl, 29 April 2021) <https://Coronamelder.nl/?utm_campaign=vws-Corona-06-2020&utm_medium=search&utm_source=bing&utm_content=ron-search-alg&utm_term=searchad-multi-device-cpc-performance> accessed 2 May 2021.

in relation to the use of special executive powers to legitimise the bypassing of ordinary parliamentary procedures. Although in Italy and the Netherlands, a law governing digital contact tracing eventually came into being, it should be noted that in none of the cases studied did the governments proactively support the introduction of regulation in parallel with the app's development. Rather, it was the political pressure exerted by opposition, civil society, DPA's and academia that paved the legislative route. In contrast, German and British officials could politically afford such resistance, although they used poor argumentation to justify their public positions. To varying degrees, the four acting prime ministers instead seemed to prefer avoiding the formal involvement of their parliaments to ensure the prompt development and launch of contact tracing tools.

A more attentive examination of clashing arguments confirms the latter observation. Within the span of a few weeks, the four acting prime ministers unrolled their strategies for contact tracing. Whether choosing to rely on public tenders or on state health authorities for the development of the apps, the common feature linking the individual procedures in the initial phase was the striking absence of parliamentary scrutiny. The main reason that seemed to push these governments' unilateral approach was the necessity of having contact tracing technology available at the ready, in light of the health infrastructure's incapacity to manually deal with the growing numbers of infections between March and May. In hindsight, the argument does not appear very solid, considering that only Italy and Germany managed to make their apps available to the public *almost* within the planned timeframe. However, even then, this was achieved at the cost of transparency (see the Italian case) and of appropriate legal safeguards (Germany still has no law). The tech-rush witnessed across Europe caused, in some circumstances, the opposite of its desired effect, with the Dutch and the UK government being forced to revert their trajectories, incurring extensive delays and, in the UK's case, the substantial waste of public funds. As pointed out across several parliamentary chambers, such mistakes could have been avoided had the ministers opened discussions with other institutions earlier. Hence, while this approach may have caused slowdowns, it would have at least ensured greater integrity in the legal and political process, as well as a more trustworthy framework for the apps.

Trust indeed appeared to be the central theme around the arguments formulated on both sides. Although governments and opposition parties, along with academia and civil society, agreed on the need to foster the trustworthiness of the apps, they largely diverged on the means to achieve this goal and on the very meaning of trust itself. In the governments' view, the level of civic trust goes hand in hand with privacy, ultimately determining a sufficient rate of use and therefore, the success of the entire policy. In practice, the Cabinets' efforts genuinely pursued the strengthening of privacy and security of the apps. In most cases, they were willing to listen to the technical recommendations of national DPA's and conduct preliminary tests on a smaller scale. Officially, the UK, Italy and Germany also switched from a centralised to a decentralised app model in order to achieve higher privacy guarantees.

However, a common feature of all debates was that the governments' attention was solely directed at the technical dimension of privacy and data protection, overlooking the broader societal implications potentially attached to the implementation of contact tracing. This was the main point of conflict with opposing and expert views. In the latter category, trust encompassed a broader range of issues revolving around the voluntariness of the apps. Besides the use of state powers to mandate download and use, experts particularly feared the intrusion of contact tracing technology in social dynamics as a pathway to horizontal discrimination and the marginalisation of the (digitally) vulnerable. Accordingly, an *ad hoc* legal basis would have therefore not only been desirable from a democratic perspective, but it would have also strengthened safeguards for voluntariness against private coercive practices, and consequently increase citizens' trust.

None of the governments seemed to share such arguments. In Germany and the UK, the health ministers and DPAs remained firmly convinced that user consent and the existing legal framework would have provided an appropriate legal basis, an argument which the respective DPAs did not dispute. Even in Italy and the Netherlands, where a legislative foundation came into being, the governments displayed a reluctant attitude. Whereas in the former case, the Cabinet deemed its vaguely phrased anti-discrimination clause fit for purpose, only in the Netherlands was a series of amendments introduced to address the social dimension of voluntariness. Again, this was not a wish voiced by government officials, but rather the result of successful political and media pressure created from critics and experts in the field.

In summary, the essence of the dispute on the need for a legal basis and on its content essentially reflects two conflicting perspectives regarding trust. The first, that of Western European governments, sees trust primarily as an objective to reach to ensure the adequate functioning of contact tracing. The second, advocated by critics and experts, envisages trust as a direct consequence of a wider process, which is of a political and legal nature. According to the latter view, trust needs to first be built in institutions and the underlying framework of the technology, rather than built on apps and their algorithms. Democratic laws should therefore be pivotal elements thereof, and not mere weights hanging off a government's storm-shaken ships.

4.5.2 The role of private tech companies

The second salient feature of the European digital contact tracing experience was the impactful role of private corporations, in particular Google and Apple. Disclosing their new Exposure Notification Framework with a joint statement in April, the Californian companies acquired de facto leadership in the realm of contact tracing technology, creating significant political consequences overseas.

Except for the Netherlands, which only drafted plans for the *CoronaMelder* at a later stage, all governments in the above case studies had to reverse their strategies in view of Google's and Apple's announcement. Although the new decentralised framework fulfilled the public's demands for stronger privacy safeguards, thus aiding governments in their quest for civic trust, it also delivered a blatant stroke to the authority of states in managing the crisis.

Italy, German and the UK offered different perspectives on how such consequences played out in the European political context. In Italy, Google's and Apple's intervention, for instance, highlighted the lack of transparency in the public procurement decision for the development of *Immuni*. In the UK, it indirectly led to delays launching the app and wasted public investment. In Germany, the state championed the centralised PEPP-PT model, triggering a tug-of-war between Merkel's Cabinet and Apple, due to the latter's unwillingness to open its interface to *CoronaWarn*. The company eventually gained the upper hand, forcing the Chancellor's team to retract its position for the sake of creating a functioning app.

What essentially was put at stake in the above circumstances was the public legitimacy of the respective ministers in their digital management of the crisis, and the consequent discrediting of their strategies in the eyes of their citizens. Ironically, those governments which tacitly chose to adapt to the tech companies' alternative framework, namely the Italian and the Dutch, suffered milder media backlash than their German and UK counterparts, which actively challenged them. Overall, this may have not played in favour of civic trust in the institutions, reiterating the growing concern for the digital sovereignty of states vis-à-vis private tech corporations.The parliamentary and inter-institutional debates that followed offered little opportunity to address the sudden access of foreign corporations to the national public health domain. In this context, it is precisely the impotency of European authorities against tech giants that seems to have fallen out of sight of the political debate's focus. On the one hand, the initial criticism advanced by some governments against Apple and Google gradually vanished into plain regret for the companies' unwillingness to cooperate in an open and transparent manner with authorities. The Italian and the German ministers of digitisation, along with other colleagues, spoke in an open letter of a "missed opportunity" for the private sector.[535] In reality, the warning disguised the white flag raised by European politicians at the conditions dictated by American tech.

By the same token, opposition in Italy, Germany, the Netherlands and the UK, did display certain concerns for the risk of personal data being accessed by Google and Apple, inviting their respective ministers to make the necessary agreements with the companies to prevent excessive power imbalances in the management of contact tracing technology at the expense of the authorities.[536] Officially, only the Dutch government pursued a similar route.[537] However, when discussions over the necessity for a legislative basis were unleashed in all four countries, there seemed to be no urge to address the prominent role of the two tech companies through democratic legislation. Of the two laws that eventually came into being, neither makes a single attempt to make the informal agreements stipulated by governments with the companies, where these occurred, into binding legal guarantees. In fact, governments and MPs across Europe seem to have overlooked the reality that both Apple and Google remain private corporations directly unaccountable to democratic oversight. Yet nothing at present prevents them from unilaterally altering their course of action independently from the demands of public authorities.

Again here, trust in (better, private) technology was considered the ultimate cure to slow political and legal processes. Adopting the privacy-friendlier decentralised framework developed by Google and Apple may have signified a positive development to the eyes of politicians and experts in contrast to the originally envisaged state-administered central servers. However, the decision came at the cost of the ever-weakening digital sovereignty of Europe and its nations, and of the central role of democratic institutions. Rather than being disappointing in hindsight, in future trajectories introducing TAGs the governance of the relationship to tech companies should be an important point of attention.

[535] Dorothee Bär and others, 'Die globalen Konzerne haben eine Chance verpasst' (faz.net, 8 June 2020) <https://www.faz.net/aktuell/politik/inland/Corona-apps-die-globalen-konzerne-haben-eine-chance-verpasst-16785681.html> accessed 2 May 2021.

[536] *See above,* Motie van der Graaf en Buitenweg (2020); *See above,* Camera dei Deputati (25 June 2020); Deutscher Bundestag, 'Antwort der Bundesregierung', (2020) Drucksache 19/21197, 5 <https://dip21.bundestag.de/dip21/btd/19/211/1921197.pdf> accessed 2 May 2021.

[537] Rijksoverheid, 'Afspraken met Google en Apple inzake Tijdelijke wet notificatieapplicatie COVID-19' (rijksoverheid.nl, 2 September 2020) <https://www.rijksoverheid.nl/documenten/publicaties/2020/09/02/afspraken-met-google-en-apple> accessed 2 May 2021.

5 Regulating the use of mobility data for public health[538]

5.1 Introduction

Framed as an indispensable component of a successful exit strategy to return from an intelligent lockdown, the Dutch government presented a temporary act (hereinafter: "proposed temporary act") on 29 May 2020 to make use of mobility data for at least six months.[539] Once adopted, the proposed temporary act would require three telecommunications providers to process mobility data, after which they would have to hand over the data via Statistics Netherlands (hereinafter: "CBS"; Dutch: *Centraal Bureau voor de Statistiek*) to the National Institute for Public Health and the Environment (hereinafter: "RIVM"; Dutch: *Rijksinstituut voor Volksgezondheid en Milieu*). The proposed temporary act has been shelved for an undetermined period of time.[540]

The proposed temporary act should not be seen in isolation but rather against the backdrop of comparable supranational and foreign initiatives. Shortly after the European Union had requested several telecommunications providers to hand over telecommunications data,[541] the European Commission released a recommendation in which it underscored the importance of using such data in the eradication of the Corona virus.[542] While the Dutch government has sought to introduce a more elaborate scheme with the proposed temporary act, other countries, including Australia[543] and France,[544] have reportedly relied upon more informal cooperation between their national authorities and national telecommunications providers.

In this article, we appraise the proposed temporary act in the light of European and Dutch telecommunications law by researching the following research question: '*Is the proposed temporary act in accordance with the principle of confidentiality introduced by the ePrivacy Directive[545] and implemented in the Dutch Telecommunications Act?*' First, we use legislative documents pertaining to the proposed temporary act to conceptualise how the Dutch government seeks to weaponize mobility data in the fight against the

[538] The research in this section was concluded in February 2021.

[539] *Parliamentary Papers II* 2019/20, 35479, nr. 2.

[540] *Parliamentary Papers II 2020/21,* 35479, nr. 1 as amended by *Parliamentary Papers II 2020/21,* 35479, nr. 8 as amended by *Parliamentary Papers II 2020/21,* 35479, nr. 11.

[541] Mark Scott, Laurens Cerulus and Laura Kayali, 'Commission tells carriers to hand over mobile data in Corona virus fight' (*Politco*, 25 March 2020) <https://www.politico.eu/article/european-commission-mobile-phone-data-thierry-breton-Corona virus-COVID19/> accessed 11 April 2021.

[542] Commission Recommendation (EU) 2020/518 of 8 April 2020 on a common Union toolbox for the use of technology and data to combat and exit from the COVID-19 crisis, in particular concerning mobile applications and the use of anonymised mobility data [2020] OJ L114/7.

[543] Ben Grubb, 'Mobile phone location data used to track Australians' movements during Corona virus crisis' (*The Sydney Morning Herald*, 5 April 2020) <https://www.smh.com.au/technology/mobile-phone-location-data-used-to-track-australians-movements-during-Corona virus-crisis-20200404-p54h09.html> accessed 11 April 2021.

[544] La Quadrature du Net, 'Orange recycles its geolocation service for the global pandemic' (*La Quadrature du Net*, 31 March 2020) <https://www.laquadrature.net/en/2020/03/31/orange-recycles-its-geolocation-service-for-the-global-pandemic/> accessed 11 April 2021.

[545] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector [2002] OJ L 201/37 as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws [2009] OJ L 337/11.

Corona virus. Second, we use the relevant provisions (and recitals[546]) in the ePrivacy Directive and the Dutch Telecommunications Act, the relevant case law from the Court of Justice of the European Union[547] (hereinafter: "Court of Justice"), and legal scholarship to discuss how the principle of confidentiality should be interpreted. In that regard, we focus on Article 15(1) ePrivacy Directive, which leaves the Member States the legislative competence to restrict the principle. Third, we apply our legal framework to our conceptual framework to examine the extent to which the proposed temporary act is in accordance with the principle of confidentiality.

Even though the proposed temporary act has been placed on hold, we seek to inform the legislative process in case the Dutch government reboots the legislative procedure. Furthermore, even though the proposed temporary act is distinct from other initiatives that concern more informal cooperation, we generalise our considerations and observations wherever possible. As such, our research could also inform (*mutatis mutandis*) discourse pertaining to using telecommunications data against the Corona virus elsewhere. More generally, we raise normative questions about the desirability of rushing to intrusive technological solutions whenever possible.

The structure of this article is as follows. First, we introduce the scheme that the proposed temporary act would erect as well as the principle of confidentiality incorporated in the ePrivacy Directive and the Dutch Telecommunications Act. Once that baseline understanding has been established, we examine to what extent the proposed temporary act satisfies the conditions set out in Article 15(1) ePrivacy Directive. We conclude by summarising our considerations and observations.

5.2 The proposed temporary act: A five-step scheme towards the weaponization of mobility data

For our purposes, the proposed temporary act would essentially erect a five-step scheme that forces three telecommunications providers to hand over mobility data via the CBS to the RIVM.[548] Once received, the RIVM needs to analyse the data to identify notable deviations in population flows. This analysis should enable the RIVM to continuously assess the effectiveness of the current control measures as well as to proactively inform the authorities about possible infection spikes.[549] In turn, the authorities could implement or reintroduce containment and mitigation measures in the hopes of finally quashing the Corona virus.[550] This scheme should essentially contribute to the Netherlands returning from an intelligent lockdown. In the subsequent subsections, we describe the proposed scheme while also flagging certain inconsistencies on a rolling basis.

5.2.1 The Minister of Economic Affairs and Minister of Health instruct telecommunications providers to hand over mobility data

In agreement with the Minister of Health, the Minister of Economic Affairs can order the three Dutch telecommunications providers to provide mobility data to the CBS.[551] Then government officials can also agree to issuing mandatory instructions on precise matters, such as how the telecommunications providers need to transfer mobility data to the CBS.[552] The Minister of Economic Affairs must first consult the telecommunications providers, the CBS, and the RIVM about any mandatory instructions to ensure that those

[546] Even though recitals are not binding on the Member States per se, they can be used to interpret (ambiguous) provisions. See Tadas Klimas and Jūraté Vaičiukaitė, 'The Law of Recitals in European Community Legislation' (2008) 15(1) ILSA Journal of International & Comparative Law 63.

[547] This article considers only case law that is readily available via CURIA, searching for the relevant provisions (and recitals) in the ePrivacy Directive.

[548] Article 14.7(1) Dutch Telecommunications Act.

[549] *Parliamentary Papers II* 2019/20, 35479, nr. 2, 3 and 4; *Parliamentary Papers II* 2019/20, 35479, nr. 7, 14.

[550] *Parliamentary Papers II* 2019/20, 35479, nr. 2, 3 and 4; *Parliamentary Papers II* 2019/20, 35479, nr. 7, 14.

[551] Article 14.7(1) Telecommiuncatiewet.

[552] Article 14.7(10) Dutch Telecommunications Act.

instructions are practical and workable.[553] This obligation for consultation has not been incorporated in the proposed temporary act. Once a mandatory instruction has been issued, the Minister of Economic Affairs can unilaterally change it.[554]

5.2.2 Telecommunications providers prepare mobility data and transfer the resulting datasets to the RIVM

Once the scheme has been launched by the Minister of Economic Affairs, the telecommunications providers need to gather mobility data from traffic and location data.[555] As a preliminary step, they need to purchase new network and information systems or reconfigure their current systems.[556] This reportedly involves the installation of one dedicated database per telecommunications provider.[557] The Dutch government has estimated preparation costs as running between € 130,240 and € 330,240 per telecommunications provider, though one can reasonably expect providers will ultimately incur different expenses due to infrastructural differences.[558] The telecommunications providers cannot claim financial compensation from the Dutch government, though the government intends to keep the preparation costs per telecommunications provider as low as possible.[559]

Expressly rejecting the idea of adopting a new data retention obligation, the Dutch government has proposed building on current business practices: the three telecommunications providers need to deduce mobility data from traffic and location data, which they already collect and store whenever a mobile device[560] actively connects to their telecommunications network.[561] Active connectivity implies that end-users use their mobile device for making phone calls, sending text messages, or roaming the internet.[562] In comparison with passive connectivity as the criterion for data collection, active connectivity leads to the collection of less traffic and location data. This difference can be attributed to end-users connecting to private networks when quarantining at home or working from the office, which cancels the need for active connectivity.[563] However, the respective mobile devices are probably still passively connected to a telecommunications network in such instances. Consequently, using active connectivity could pose issues to the effectiveness of the scheme in the sense that collected traffic and location data could represent only a partial view of the whole population flow picture. Furthermore, the telephone number and international mobile subscriber identity of actively connected mobile devices, the identification number of connected antennae, and the starting and ending time of respective connections are all examples of traffic and location data.[564]

Pursuant to the proposed temporary act, mobility data consists of the total number of mobile devices per municipality and per hour that have been actively connected to one of the telecommunications provider's networks within the respective municipality and during the respective hour.[565] That number is broken down by the municipality of origin of the mobile devices.[566] For our purposes, telecommunications

[553] *Parliamentary Papers II* 2019/20, 35479, nr. 7, 36 and 42.

[554] Article 14.7(10) Dutch Telecommunications Act.

[555] Article 14.7(1) Dutch Telecommunications Act.

[556] *Parliamentary Papers II* 2019/20, 35479, nr. 2, 8; *Parliamentary Papers II* 2019/20, 35479, nr. 7, 40.

[557] Nando Kasteleijn, 'Privacywaakhond: huidig wetsvoorstel telecomdata delen RIVM niet invoeren' (NOS Nieuws, 3 July 2020) <https://nos.nl/artikel/2339365-privacywaakhond-huidig-wetsvoorstel-telecomdata-delen-rivm-niet-invoeren.html> accessed 11 April 2021.

[558] *Parliamentary Papers II* 2019/20, 35479, nr. 2, 8; *Parliamentary Papers II* 2019/20, 35479, nr. 7, 52.

[559] *Parliamentary Papers II* 2019/20, 35479, nr. 7, 42 and 52-53.

[560] Not only smart phones but also tablets, cars, and other devices fitted with a sim card are mobile devices in this context.

[561] Articles 14.7(2), 14.7(3) and 11.5(2) Dutch Telecommunications Act; *Parliamentary Papers II* 2019/20, 35479, nr. 2, 11; *Parliamentary Papers II* 2019/20, 35479, nr. 7, 8; *Parliamentary Papers II* 2020/21, 35479, nr. 10, 2 and 5; *Parliamentary Papers II* 2020/21, 35479, nr. 11, 3.

[562] *Parliamentary Papers II* 2019/20, 35479, nr. 2, 5-6; *Parliamentary Papers II* 2019/20, 35479, nr. 7, 8; *Parliamentary Papers II* 2020/21, 35479, nr. 10, 2 and 5; *Parliamentary Papers II* 2020/21, 35479, nr. 11, 3.

[563] Besides, an end-user may not call or text on an hourly basis because services such as WhatsApp and email allow them to communicate via their private networks, and because an end-user may not have purchased a roaming subscription.

[564] *Parliamentary Papers II* 2019/20, 35479, nr. 2, 5, 6 and 10; *Parliamentary Papers II* 2019/20, 35479, nr. 7, 8.

[565] Article 14.7(2) Dutch Telecommunications Act.

[566] Article 14.7(2) Dutch Telecommunications Act.

providers need to perform the following four sets of processing operations in order to deduce mobility data from collected traffic and location data.

5.2.2.1 Preparing traffic and location data for processing

First, telecommunications providers need to strip traffic and location data from identifying information.[567] That processing operation leaves the country code of connected mobile devices, the identification number of connected antennae, and the starting time of respective connections untouched.[568] Furthermore, telecommunications providers need to encrypt and pseudonymise that data in an effort to preserve end-user privacy in as much as possible.[569]

5.2.2.2 Determining the hourly location of mobile devices

Second, telecommunications providers need to determine the municipality, or municipalities, in which mobile devices were actively connected, broken down by hour.[570] In that regard, they need to base these on the identification numbers of connected antennae.[571] This approach can result in inaccuracies around municipal peripheries because antenna coverage does not follow municipal borders neatly.[572] Attempting to resolve this issue from the outset, the Dutch government has proposed assigning every antenna to one or more municipalities in advance. Furthermore, it has noted that the CBS will estimate per antenna the probability of a mobile device actively connecting to it from one or more surrounding municipalities.[573] Those estimations are then used to assign antennae to one or more municipalities, and telecommunications providers need to use the resulting grid for the purposes of the scheme.

Suppose that the CBS estimated that the probability of a mobile device actively connecting to antenna 19191 from Haarlemmermeer is 40%, from Amstelveen is 30%, and from Amsterdam is also 30%. Furthermore, suppose that the data show that 5,000 mobile devices were connected to antenna 19191 for an hour. The respective telecommunications provider would then conclude that 2,000 mobile devices were in Haarlemmermeer, 1,500 mobile devices were in Amstelveen, and 1,500 mobile devices were in Amsterdam during that hour. Framed as adding statistical noise, the Dutch government has noted that this processing operation contributes to preserving end-user privacy.[574]

Furthermore, deducing mobility data from traffic and location data becomes more complicated when a mobile device has been actively connected to antennae in different municipalities for an hour. Then, the respective telecommunications provider needs to determine the most relevant municipality in which the mobile device was during that hour, after which it should register only that location with the mobile device's pseudonym. In that regard, the respective telecommunications provider needs to use an undetermined method to correct for biases and inaccuracies, such as intermunicipal commuting by train. [575] The Dutch government has noted that the CBS will support telecommunications companies by developing an optimised method for each of them.[576]

Suppose that the data show that a mobile device was connected to antenna 16621 in Amsterdam, antenna 45681 in Lansingerland, and antenna 66751 in Rotterdam for an hour. The respective telecommunications provider's optimised method would then decide whether Amsterdam, Lansingerland, or Rotterdam was the most relevant municipality in which the mobile device had been during that hour.

[567] *Parliamentary Papers II* 2019/20, 35479, nr. 7, 8.
[568] *Parliamentary Papers II* 2019/20, 35479, nr. 7, 8.
[569] *Parliamentary Papers II* 2019/20, 35479, nr. 7, 8.
[570] Article 14.7(2) Dutch Telecommunications Act.
[571] *Parliamentary Papers II* 2019/20, 35479, nr. 7, 8, 30 and 31.
[572] *Parliamentary Papers II* 2019/20, 35479, nr. 7, 8, 30 and 31.
[573] Article 14.7(3) Dutch Telecommunications Act; *Parliamentary Papers II* 2020/21, 35479, nr. 10, 3.
[574] *Parliamentary Papers II* 2020/21, 35479, nr. 10, 2 and 4.
[575] *Parliamentary Papers II* 2019/20, 35479, nr. 7, 8 and 39.
[576] *Parliamentary Papers II* 2019/20, 35479, nr. 7, 8 and 39.

Moreover, when a mobile device was not actively connected to any antenna for an hour, the respective telecommunications provider can neither determine in which municipality the device was nor register a location with the device's pseudonym.[577] According to the Dutch government, the CBS would have to correct such biases and inaccuracies.[578]

As soon as they have determined a connected mobile device's hourly location, the telecommunications providers need to strip the data from the identification numbers of connected antennae. This leaves only the country code of connected mobile devices and the starting time of respective connections untouched.[579]

5.2.2.3 Determining a mobile device's municipality of origin

Third, telecommunications providers need to determine the connected mobile device's municipality of origin, or an end-user. In that regard, telecommunications providers need to distinguish between mobile devices with a domestic country code and those with a foreign one.

With respect to domestic country codes, telecommunications providers need to base themselves on a connected mobile device's hourly location over the past thirty days. This processing operation involves the telecommunications providers storing hourly locations for no longer than 30 days, which could theoretically result in the registration of 720 data points per mobile device. The municipality in which a mobile device is registered most often over the past 30 days is deemed the device's municipality of origin for purposes of the proposed temporary act.[580]

Suppose that a mobile device was registered as being in Amsterdam 365 times and in Rotterdam 355 times over the past 30 days. The respective telecommunications provider would then need to designate Amsterdam as the mobile device's municipality of origin on day 31. Now suppose that on day 31 the mobile device was registered as being in Amsterdam 345 times and in Rotterdam 375 times over the past 30 days. The respective telecommunications provider would then need to designate Rotterdam as the mobile device's municipality of origin on day 32.

As soon as they have determined the municipality of origin, telecommunications providers need to delete the connected mobile devices' hourly locations older than 30 days from the data.[581] Based on legislative documents, we cannot ascertain what they should do with the country code of connected mobile devices and the starting times of respective connections.

With respect to foreign country codes, telecommunications providers need to equate a connected mobile device's municipality of origin with their country code.[582] The Dutch government has identified nine categories of foreign country codes: Germany, Belgium, the United Kingdom, other countries in Europe, countries in North America, countries in South America, countries in Asia, countries in Africa, and countries in Oceania.[583] Telecommunications providers should delete foreign country codes from the data as soon as they have handed the resulting mobility data over to the CBS.[584] However, such a data destruction obligation has not been incorporated in the proposed temporary act.

5.2.2.4 Deducing mobility data from traffic and location data

[577] *Parliamentary Papers II* 2019/20, 35479, nr. 7, 8.

[578] *Parliamentary Papers II* 2019/20, 35479, nr. 2, 4; *Parliamentary Papers II* 2019/20, 35479, nr. 7, 20, 29 and 31; *Parliamentary Papers II* 2020/21, 35479, nr. 10, 5.

[579] *Parliamentary Papers II* 2019/20, 35479, nr. 2, 10; *Parliamentary Papers II* 2019/20, 35479, nr. 7, 8.

[580] Article 14.7(4)(1) Dutch Telecommunications Act. The data used to deduce the municipality of origin include location data, antennae maps, land use maps, and public geographical information. See *Parliamentary Papers II* 2019/20, 35479, nr. 2, 5.

[581] Article 14.7(7) Dutch Telecommunications Act.

[582] Article 14.7(4)(2) Dutch Telecommunications Act.

[583] Article 14.7(4)(2) Dutch Telecommunications Act.

[584] *Parliamentary Papers II* 2019/20, 35479, nr. 7, 9.

Fourth, telecommunications providers need to determine the total number of mobile devices per municipality and per hour that were actively connected to their network within the respective municipality and during the respective hour, broken down by the connected mobile device's municipality of origin.[585] Subsequently, they need to aggregate the resulting mobility data in a table, as well as discard any total number less than 15 to preserve end-user privacy as much as possible.[586] Finally, they need to transfer 24 mobility data tables to the CBS once daily.[587]

5.2.3 The CBS consolidates and cleans the data and shares it with the RIVM

Once telecommunications providers have transferred the mobility data tables, the CBS needs to consolidate the individual tables and delete them.[588] Then, it needs to correct for biases and inaccuracies like the number of mobile devices not actively connected to antennae for an hour.[589] Furthermore, it needs to convert mobility data pertaining to mobile devices into mobility data pertaining to end-users.[590] In that regard, it can combine consolidated mobility data tables with other datasets, among other things.[591] While such methods have not yet been determined, the Dutch government has stated that it aspires to be transparent as much as possible, having noted that the CBS will need to make public a technical description of its methods.[592] However, such a transparency requirement is missing in the proposed temporary act. Furthermore, the CBS needs to round mobility data to the nearest 50 to contribute to preserving end-user privacy.[593]

Subsequently, the CBS could draft a report accompanying the data, which could provide an overview of the most notable intermunicipal movements.[594] Finally, it needs to transfer the processed consolidated mobility data tables and the accompanying reports to the RIVM.[595] While the RIVM can specify the format and frequency of such data transfers, the CBS remains independent in determining its methods.[596]

Considering that statistical errors can occur when processing consolidated data, the CBS can store the data, whether processed or not, for as long as needed for the RIVM to fight the Corona virus in order to correct for such errors.[597] However, it cannot store the tables longer than one year from when telecommunications providers transferred the underlying mobility data tables.[598] Meanwhile, it can neither process the consolidated data for purposes other than assisting the RIVM nor share the data with entities other than the RIVM.[599] Furthermore, the CBS must implement the necessary technical and organisational measures to ensure the security of the consolidated data.[600]

5.2.4 The RIVM checks the data for notable deviations

Once the CBS has transferred processed mobility data tables and, where appropriate, accompanying reports, the RIVM needs to analyse the data in the hopes of achieving the following two objectives. First, it should be able to use the data to continuously assess the effectiveness of the control measures in force.[601] Second, it should be able to use the data to proactively inform the municipalities, the municipal

[585] Article 14.7(2) Dutch Telecommunications Act.
[586] Article 14.7(5) Dutch Telecommunications Act.
[587] Article 14.7(6) Dutch Telecommunications Act.
[588] Article 14.7(9) Dutch Telecommunications Act.
[589] *Parliamentary Papers II* 2019/20, 35479, nr. 2, 4; *Parliamentary Papers II* 2019/20, 35479, nr. 7, 22 and 30-11; *Parliamentary Papers II* 2020/21, 35479, nr. 10, 5.
[590] *Parliamentary Papers II* 2019/20, 35479, nr. 7, 7, 33 and 34.
[591] *Parliamentary Papers II* 2019/20, 35479, nr. 2, 4; *Parliamentary Papers II* 2019/20, 35479, nr. 7, 11 and 22.
[592] *Parliamentary Papers II* 2019/20, 35479, nr. 2, 4; *Parliamentary Papers II* 2019/20, 35479, nr. 7, 11 and 34.
[593] *Parliamentary Papers II* 2020/21, 35479, nr. 10, 5.
[594] *Parliamentary Papers II* 2019/20, 35479, nr. 2, 4; *Parliamentary Papers II* 2019/20, 35479, nr. 7, 11 and 34.
[595] Article 14.7(8) Dutch Telecommunications Act.
[596] *Parliamentary Papers II* 2019/20, 35479, nr. 2, 9.
[597] Article 14.7(9) Dutch Telecommunications Act.
[598] Article 14.7(9) Dutch Telecommunications Act.
[599] Articles 14.7(1) and 14.7(8) Dutch Telecommunications Act.
[600] Article 38 Wet op het Centraal bureau voor de statistiek; *Parliamentary Papers II* 2019/20, 35479, nr. 7, 13 and 29.
[601] Article 14.7(1) Dutch Telecommunications Act; *Parliamentary Papers II* 2019/20, 35479, nr. 2, 3 and 4; *Parliamentary Papers II* 2019/20, 35479, nr. 7, 14.

health services, the security regions, and the Minister of Health about the possible resurgence of the Corona virus, which could lead to the implementation or reintroduction of containment and mitigation measures at the national, regional or local level.[602]

The Dutch government anticipates that the RIVM could deduce trends in Dutch end-users' intermunicipal movements and foreign end-users' intrastate movements from the datasets.[603] In that regard, the RIVM can combine the dataset with other datasets like positive test results per municipality, among other things.[604] As was noted previously, it should publish a technical description of its methods, but such a transparency requirement has not been incorporated in the proposed temporary act.[605] Furthermore, the Dutch government expects that the RIVM could use the data to map which municipalities of origin are the municipalities with the most intermunicipal movement per day.[606] Moreover, it forecasts that the RIVM could use the data to predict the infection risk per municipality, as well as rank municipalities contributing the most to the spread of the Corona virus.[607]

Furthermore, the RIVM needs to notify the municipalities, the municipal health services, and the security regions as soon as it has identified any notable deviation in intermunicipal movement. Furthermore, it needs to notify the Minister of Health when such a deviation is significant.[608] When sending out notifications, it should be careful not to share data with the authorities.[609] Rather, it should make sure that the authorities cannot even deduce mobility data from the notification.[610] However, such a safeguard is missing from the proposed temporary act.

Like the CBS, the RIVM can store the data for as long as needed in the fight against the Corona virus, though no longer than one year from when the telecommunications providers transfer the underlying mobility data tables to the CBS.[611] Meanwhile, it is legally prohibited from processing the data for purposes other than eradicating the Corona virus.[612] Furthermore, it should implement measures to ensure the security of the mobility data,[613] but such a cybersecurity requirement has purposefully not been incorporated in the proposed temporary act nor in other legal frameworks.

5.2.5 Public authorities intervene when necessary

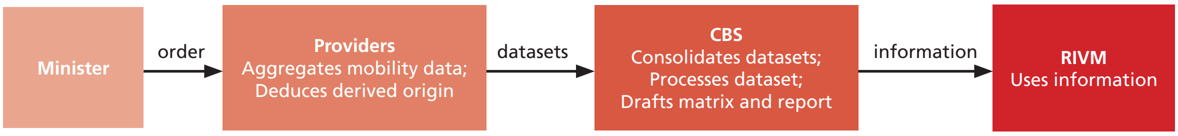
Once the RIVM has notified them, the municipalities, municipal health services, security regions, and the Minister of Health can proactively implement or reintroduce control and mitigation measures at the national, regional, or local level. Discouraging individuals to visit regions and locations like municipalities, prioritising outbreak investigations, and giving a prognosis for the infection risk are examples of possible actions.[614] According to the Dutch government, such actions will be determined predominantly by local authorities,[615] and the proposed scheme essentially functions as a warning system.[616] Furthermore, local and regional authorities can also reach out to the RIVM on their own initiative.[617]

[602] Article 14.7(1) Dutch Telecommunications Act; *Parliamentary Papers II* 2019/20, 35479, nr. 2, 3 and 4; *Parliamentary Papers II* 2019/20, 35479, nr. 7, 14.
[603] *Parliamentary Papers II* 2019/20, 35479, nr. 7, 14.
[604] *Parliamentary Papers II* 2019/20, 35479, nr. 7, 26.
[605] *Parliamentary Papers II* 2019/20, 35479, nr. 7, 11.
[606] *Parliamentary Papers II* 2019/20, 35479, nr. 7, 11, 14, 15 and 26.
[607] *Parliamentary Papers II* 2019/20, 35479, nr. 7, 11, 14, 15 and 26.
[608] *Parliamentary Papers II* 2019/20, 35479, nr. 7, 20.
[609] *Parliamentary Papers II* 2019/20, 35479, nr. 7, 29.
[610] *Parliamentary Papers II* 2019/20, 35479, nr. 2, 10 and 11.
[611] Article 14.7(9) Dutch Telecommunications Act.
[612] Article 14.7(1) Dutch Telecommunications Act.
[613] *Parliamentary Papers II* 2019/20, 35479, nr. 7, 30.
[614] *Parliamentary Papers II* 2019/20, 35479, nr. 7, 30, 17 and 28.
[615] *Parliamentary Papers II* 2019/20, 35479, nr. 7, 11, 17 and 28.
[616] *Parliamentary Papers II* 2019/20, 35479, nr. 7, 32, 34 and 42.
[617] *Parliamentary Papers II* 2019/20, 35479, nr. 7, 54.

5.2.6 Interim conclusion

The following graphic depiction summarises the foregoing description of the mechanism presented in the legislative proposal.

Figure 2. Interplay of different stakeholders and steps in the proposal



5.3 The ePrivacy Directive and the Dutch Telecommunications Act: Vehicles towards the protection of privacy and personal data

The ePrivacy Directive is a sector-specific legal framework[618] with a dual objective.[619] On the one hand, the ePrivacy Directive is designed to protect fundamental rights, especially those of privacy and data protection, enshrined in the Charter of the Fundamental Rights of the European Union (hereinafter: "CFREU").[620] On the other hand, the ePrivacy Directive helps establish the internal market for telecommunications networks and services.[621] The ePrivacy Directive attempts to achieve those objectives by regulating the processing of personal data only in the telecommunications sector.[622] The Dutch government has implemented the ePrivacy Directive provisions in the Dutch Telecommunications Act: the *Telecommunicatiewet*.

5.3.1 The scope of application of the European and Dutch telecommunications law

The ePrivacy Directive and the Dutch Telecommunications Act regulate the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks.[623] Put differently, the subject matter of the Dutch Telecommunications Act comprises four conditions: public communications networks, publicly available electronic communications services, personal data, and processing.

Public communications networks are transmission systems that permit the conveyance of signals by electromagnetic means, including mobile networks.[624] In the Netherlands, there are three major providers of public communications networks (hereinafter: "network operators") operating on the domestic market: KPN, Vodafone, and T-Mobile.[625] In turn, publicly available electronic communications services involve the transmission of signals over electronic communications networks.[626] There are many more providers of publicly available electronic communications services (hereinafter: "service providers") active on the Dutch telecommunications market.[627] Service providers are not necessarily network operators, though in the Netherlands, the three major network operators also provide electronic communications services. Hereinafter, we use the notion "telecommunications providers" to refer to both network operators and service providers.

[618] Article 1 ePrivacy Directive.

[619] Joris van Hoboken and Frederik Zuiderveen Borgesius, 'Scoping Electronic Communication Privacy Rules: Data, Services and Values' (2015) 6(3) Journal of Intellectual Property, Information Technology and E-Commerce Law 198, 199; Frederik Zuiderveen Borgesius, Joris van Hoboken, Ronan Fahy, Kristina Irion and Max Rozendaal, 'An assessment of the Commission's Proposal on Privacy and Electronic Communications. Study for the LIBE Committee' (2017) 23.

[620] Charter of the Fundamental Rights of the European Union [2012] OJ C 326/391.

[621] Recitals 5 and 8 ePrivacy Directive.

[622] Article 3 ePrivacy Directive. The ePrivacy Directive does not aspire full harmonisation. See recital 8 ePrivacy Directive.

[623] Article 11.2 Dutch Telecommunications Act; Article 3 ePrivacy Directive.

[624] Article 1.1 Dutch Telecommunications Act; Article 2 ePrivacy Directive in conjunction with Article 2(1) Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (Recast) [2018] OJ L 321/36 (hereinafter: European Electronic Communications Code).

[625] Autoriteit Consument & Markt, 'Leidraad. Delen van mobiele netwerken. Concept' (2020) 4.

[626] Article 1.1 Dutch Telecommunications Act; Article 2 ePrivacy Directive in conjunction with Article 2(4) European Electronic Communications Code.

[627] Autoriteit Consument & Markt, 'Leidraad. Delen van mobiele netwerken. Concept' (2020) 4.

Provided that the Dutch Telecommunications Act is a *lex specialis* to the General Data Protection Regulation,[628] the notions of "personal data" and "processing" must be construed in accordance with the latter legal framework.[629] Any information relating to an identified as well as identifiable natural person, the data subject, should be considered personal data,[630] and any automatic set of operations performed on personal data should be considered processing[631]. Both notions must be construed broadly.[632] For our purpose, the CJEU has repeatedly concluded that telecommunications providers process traffic and location data within the context of providing their services, and that traffic and location data should be considered personal data.[633] The General Data Protection Regulation lists location data as an example of personal data.[634]

More specifically, traffic data are "data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof."[635] Examples include "data referring to the routing, duration, time or volume of a communication, to the protocol used, to the location of the terminal equipment of the sender or recipient, to the network on which the communication originates or terminates, [and] to the beginning, end or duration of a connection."[636] Location data are "data processed in a public electronic communications network or by a publicly available electronic communications service", which indicate the geographic position of the terminal equipment of a user of such a service.[637]

5.3.2 The principle of confidentiality in European and Dutch telecommunications law

The Dutch Telecommunications Act dictates that telecommunications providers need to ensure the confidentiality of communications and related traffic data by means of their networks and services.[638] In that connection, telecommunications providers should refrain from tapping, eavesdropping, or other kinds of interception or surveillance of communications and related traffic data without the end-user's consent or another legal basis.[639] Put differently, end-users can rest assured that their communications and related traffic data remain anonymous or are not recorded, unless they have agreed otherwise.[640]

[628] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC [2016] OJ L119/1.

[629] Articles 1(2) and 2 ePrivacy Directive in conjunction with Article 95 General Data Protection Regulation. See Frederik Zuiderveen Borgesius, Joris van Hoboken, Ronan Fahy, Kristina Irion and Max Rozendaal, 'An assessment of the Commission's Proposal on Privacy and Electronic Communications. Study for the LIBE Committee' (2017) 23-25; European Data Protection Board, 'Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities' (2019) 5-16; Piedade Costa de Oliveira, 'Article 95. Relationship with Directive 2002/58/EC' in Christopher Kuner, Lee A. Bygrave and Christopher Docksey (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press 2020).

[630] Article 4(1) General Data Protection Regulation.

[631] Article 4(2) General Data Protection Regulation.

[632] Chris Jay Hoofnagle, Bart van der Sloot and Frederik Zuiderveen Borgesius, 'The European Union general data protection regulation: what it is and what it means' (2019) 28(1) Information & Communications Technology Law 65, 72 and 73; Lee A. Bygrave and Luca Tosoni, 'Article 4(1). Personal data' in Christopher Kuner, Lee A. Bygrave and Christopher Docksey, *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press 2020) 113 and 114; Luca Tosoni and Lee A. Bygrave, 'Article 4(2). Processing' in Christopher Kuner, Lee A. Bygrave and Christopher Docksey, *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press 2020) 119.

[633] *Privacy International*, paras 40 and 41.

[634] Article 4(1) General Data Protection Regulation.

[635] Article 11.1(b) Dutch Telecommunications Act; Article 2(b) ePrivacy Directive.

[636] Recital 15 ePrivacy Directive.

[637] Article 11.1(d) Dutch Telecommunications Act; Article 2(c) ePrivacy Directive.

[638] Article 11.2a(1) Dutch Telecommunications Act; Article 5(1) ePrivacy Directive.

[639] Article 11.2a(2) Dutch Telecommunications Act; Article 5(1) ePrivacy Directive. Dutch telecommunications providers can set aside this general prohibition, for example, to ensure, where necessary, the integrity and security of their networks or services, to convey communications by means of their networks or services, or to give effect to a statutory provision or a court order. See Article 11.2a(2) Dutch Telecommunications Act; Article 5(1) ePrivacy Directive.

[640] *Privacy International*, para 57; *La Quadrature du Net*, para 109.

The principle of confidentiality is protected further in other provisions. Most importantly, telecommunications providers cannot store or process traffic and location data, unless an exception like consent applies.[641] To digress slightly, other Member States like France most likely have their telecommunications providers rely on such an exception in order to facilitate the exchange of telecommunications data between their authorities and telecommunications providers for the purposes of eradicating the Corona virus. The Dutch government has chosen another path, namely that of Article 15(1) ePrivacy Directive, which leaves Member States with the legislative competence to restrict the principle of confidentiality, provided that three conditions have been satisfied.[642]

5.3.3 The fundamental rights dimension of European and Dutch telecommunications laws

The ePrivacy Directive and the Dutch Telecommunications Act should protect fundamental rights, especially the fundamental rights to privacy[643] and data protection, as enshrined in the Charter.[644] The European Court of Justice has repeatedly underlined this fundamental rights dimension. Whereas the fundamental right to privacy dictates that "[everyone] has the right to respect for his or her private and family life, home and communications",[645] the right to data protection mandates that "[everyone] has the right to the protection of personal data concerning him or her".[646] Against that backdrop, the principle of confidentiality and its practical implementation can be framed as vehicles towards the protection of fundamental rights.

But fundamental rights are not absolute. The Charter allows interference with fundamental rights when three conditions have been met. First, the interference must be provided for by law.[647] Second, it must respect the essence of the affected fundamental rights.[648] Third, it must comply with the principle of proportionality, which requires that interference is necessary and genuinely meets the objective of general interests or is needed to protect others' fundamental rights.[649]

5.4 The proposed temporary act in the light of Art 15(1) ePrivacy Directive

The proposed temporary act essentially introduces a five-step scheme to force KPN, Vodafone, and T-Mobile to process location and traffic data in order to deduce mobility data from them. The Dutch Telecommunications Act regulates only the second step, as the other steps involve neither network operators nor service providers. Steps three to five would be governed by the General Data Protection Regulation to the extent that they concern the processing of personal data.[650] We will focus on the second step and to keep the scope of our article manageable, we have not researched the application of the General Data Protection Regulation to other steps.

[641] Articles 11.5 and 11.5a Dutch Telecommunications Act; Articles 6 and 9 ePrivacy Directive. Dutch telecommunications providers can, for example, process *traffic data* only to the extent necessary for the transmission of communications, provided that they erase or anonymise the traffic data as soon as possible. See Article 11.5 Dutch Telecommunications Act: Article 6 ePrivacy Directive. Additionally, Dutch telecommunications providers can, for example, process *location data* other than traffic data only to the extent the data has been anonymised, provided that the processing of the data location is restricted to persons acting under their authority. See Article 11.5a Dutch Telecommunications Act; Article 9 ePrivacy Directive. We do not research these exceptions further.

[642] The Dutch legislature has called on the legislative competence to adopt exceptions for purposes of national security as well as the prevention, detection, and prosecution of criminal offences. See Article 11.13 Dutch Telecommunications Act. We do not consider those specific exceptions further.

[643] Article 7 Charter. To be sure, while the Charter formally includes a fundamental right to respect for private and family life, we speak of the fundamental right to privacy to draw attention to the right to confidentiality of communications as well as for readability purposes. Compare Gloria González-Fuster, *The emergence of personal data protection as a fundamental right of the EU* (Springer 2014) 81-84 and 255.

[644] Article 1 ePrivacy Directive; Article 11.2 Dutch Telecommunications Act.

[645] Article 7 Charter.

[646] Article 8(1) Charter.

[647] Article 52(1) Charter.

[648] Article 52(1) Charter.

[649] Article 52(1) Charter.

[650] European Data Protection Board, 'Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak' (2020) 5 and 6.

As it currently stands, the Dutch Telecommunications Act does not allow the three telecommunications providers to process traffic and location data for purposes of the five-step scheme.[651] This means that the proposed temporary act would require telecommunications providers to systematically breach the principle of confidentiality, were it not that the Dutch government aims to incorporate an exception in the proposed temporary act in the hopes of legitimising such processing operations conducted during the second step. The Dutch government has explicitly called on Article 15(1) ePrivacy Directive, which awards it the legislative competence to restrict the principle of confidentiality, provided that three conditions have been satisfied.[652] First, the restriction needs to take the form of a legislative measure.[653] Second, it needs to safeguard the general interest. Third, it needs to be a necessary, appropriate, and proportionate measure within democratic society. Hereinafter, we examine the extent to which the proposed temporary act complies with the second and third conditions. We do not consider compliance with the first condition, as it seems evident that the proposed temporary act should be classified as a legislative measure.[654]

5.4.1 Article 15(1) ePrivacy Directive: A legal primer

Before we examine the extent to which the proposed temporary act meets the conditions of Article 15(1) ePrivacy Directive, we will make some preliminary observations pertaining to the interpretation of the provision in order to create a baseline understanding. First, the European Court of Justice has elucidated that Article 15(1) ePrivacy Directive must be strictly interpreted.[655] In that regard, an exception to the principle of confidentiality cannot become the standard rule, as that would render the principle largely meaningless.[656] Second, the European Court of Justice has underlined that Article 15(1) ePrivacy Directive should be interpreted in the light of the Charter, as any restriction needs to be in accordance with general principles of unitary law, including the Charter.[657] In that vein, it has repeatedly held that a derogation from or a limitation to the fundamental right to privacy can only be made to the extent that it is strictly necessary.[658] Moreover, recital 11 ePrivacy Directive specifies that any restriction needs to be strictly proportionate to the intended purpose, and Article 15(1) ePrivacy Directive mandates that data retention legislation is justified with reference to general interests and limited in duration.[659] By and large, the conditions of Article 15(1) ePrivacy Directive are a high bar to clear.

[651] The telecommunications providers can process *traffic data* only to the extent necessary for the transmission of communications, and they must erase or anonymise data as soon as possible. However, the processing of data needs to be restricted to persons acting under their authority handling billing or traffic management, customer enquiries, fraud detection, or market research or sales activities relating to their services or providing value-added services. The processing of data needs to be restricted to what is necessary for purposes of such activities. See Article 11.5 Dutch Telecommunications Act; Article 6 ePrivacy Directive. The telecommunications providers can process *location data* other than traffic only to the extent the data has been anonymised, though the processing of the data must be restricted to persons acting under their authority. See Article 11.5a Dutch Telecommunications Act; Article 9 ePrivacy Directive. Those exceptions would not facilitate the Dutch government in using telecommunications data in the fight against the Corona virus due to legal and practical reasons.

[652] *Parliamentary Papers II* 2019/20, 35479, nr. 2, 5. In the Netherlands, the legislation has already called on the legislative competence to provide exceptions to provisions on traffic and location data for purposes of national security, as well as the prevention, detection and prosecution of criminal offences. See Article 11.13 Dutch Telecommunications Act. We will not consider these specific exceptions further as doing so is irrelevant for our purposes.

[653] This condition needs to be construed narrowly in the sense that the restriction should have a formal legal basis, meaning it cannot be grounded in substantive legal bases, such as with case law or unwritten law. See Wilfred Steenbruggen, *Publieke dimensies van privé-communicatie: een onderzoek naar de verantwoordelijkheid van de overheid bij de bescherming van vertrouwelijke communicatie in het digitale tijdperk* (Otto Cramwinckel Uitgever 2009) 189.

[654] We would like to commend the Dutch government for its efforts. Even though it needs to adopt the proposed temporary act to facilitate the five-step scheme, the preceding legislative procedure would have undermined democratic oversight and the democratic legitimisation of the proposed temporary act, as well as the scheme it would erect. This should be contrasted with the approaches of other Member States towards using telecommunications data, which seem to have predominantly relied on cooperation between national authorities and national telecommunications providers.

[655] *Tele2*, para 89.

[656] *Tele2*, para 89; *Privacy International*, paras 59 and 69; *La Quadrature du Net*, paras 111 and 142.

[657] *Tele2*, para 91; *Privacy International*, paras 60, 62 and 63; *La Quadrature du Net*, paras 113, 114 and 120-128. See Article 15(1) ePrivacy Directive; section 1.3.3.

[658] *Tele2*, para 96; *Privacy International*, para 67; *La Quadrature du Net*, para 130.

[659] *Tele2*, para 95; *Privacy International*, paras 66 and 67; *La Quadrature du Net*, paras 129 and 130.

5.4.2 The proposed temporary act: A notably serious interference with the fundamental right to privacy and data protection

The Dutch government has called on Article 15(1) ePrivacy Directive to adopt an exception that would allow three telecommunications providers to lawfully process location and traffic data, which would otherwise have been prohibited under the Dutch Telecommunications Act.[660] In that sense, the mere adoption of the proposed temporary act would constitute an interference with the principle of confidentiality, as well as underlying fundamental rights.[661] Before we examine the extent to which the proposed temporary act clears the bar of Article 15(1) ePrivacy Directive, we will classify and elaborate on how serious this interference is to fundamental rights. The seriousness of this interference has important consequences under Article 15(1) ePrivacy Directive: the more serious the interference, the more stringent the conditions.[662] For our purposes, the following four factors suggest that the proposed temporary act needs to be classified as a notably serious interference with fundamental rights.

First, telecommunications providers have to process the personal data of millions of individuals over a period of no less than six months. We consider location and traffic data, as well as mobility data, to be personal data within the meaning of Article 4(1) General Data Protection Regulation.[663] The media has already speculated that providers would need to process the personal data of around twelve million individuals, which is roughly 69% of the total Dutch population.[664]

From a legal perspective, the European Court of Justice has considered it instructive to consider whether the data, taken as a whole, allow precise conclusions to be drawn about the private lives of the individuals concerned and provide a means to profile them.[665] Because of the amounts of personal data being collected, the duration for which it is being collected, and the duration of the proposed temporary act, among other things, the five-step scheme would definitely result in the collection and storage of data that allows for such conclusions to be drawn and such profiles to be created.[666] Suppose that the hourly locations of a mobile device show that it originates in a strictly religious municipality and that it is frequently taken to a municipality known for its gay meeting sites. The respective telecommunications provider could then use the data to draw conclusions about the respective end-user's religious beliefs and sexual identity, which are special categories of personal data.[667]

Second, the proposed temporary act does not provide the millions of concerned individuals with a meaningful option to dissent in having their personal data processed for the purposes of the five-step scheme.[668] Considering that their traffic and location data will be collected and stored whenever they actively connect to a telecommunications network, the only thing those individuals can do is switch their mobile devices to airplane mode, or leave their devices at home or at the office.[669] In that regard, one can argue that is undesirable that individuals do so in view of the expedient dissemination of Corona virus-related news as well as the efficacious functioning of the CoronaMelder application, the Dutch government's contact tracing application.

[660] *Parliamentary Papers II* 2019/20, 35479, nr. 2, 5 and 10.

[661] Compare *Tele2*, paras 99-101; *Ministerio Fiscal*, paras 59-61; *La Quadrature du Net*, paras 115, 116 and 118. By analogy, see *Digital Rights Ireland*, paras 25-30.

[662] See sections 1.4.3 and 1.4.4.

[663] *Parliamentary Papers II* 2019/20, 35479, nr. 2, 6 and 10; *Parliamentary Papers II* 2020/21, 35479, nr. 11, 3.

[664] Jeroen Piersma en Martijn Pols, 'KPN weigerde locatiedata van klanten met Brussel te delen' *Het Financieele Dagblad* (Amsterdam, 30 June 2020) 12; 'Telecomdata verzamelen is riskante stap' *Het Financieele Dagblad* (Amsterdam, 1 July 2020) 5.

[665] Compare *Tele2*, para 99; *Ministerio Fiscal*, paras 59-60; *Privacy International*, para 71; *La Quadrature du Net*, para 117. By analogy, see *Digital Rights Ireland*, paras 26-27.

[666] Compare *Privacy International*, para 72.

[667] Article 9(1) General Data Protection Regulation. When personal data fall within a special category, the General Data Protection Regulation calls for a higher level of protection because the processing of such data could present more serious risks to the data subject's fundamental rights and freedoms. See recital 51 General Data Protection Regulation. In contrast to ordinary categories of personal data, special categories of personal data can only be processed in exceptional circumstances, such as when the data subject has given their explicit consent. See Article 9(2) General Data Protection Regulation. Compare Privacy International, para 73; La Quadrature du Net, paras 117 and 142.

[668] 'Telecomdata verzamelen is riskante stap' *Het Financieele Dagblad* (Amsterdam, 1 July 2020) 5.

[669] See section 1.2.2. Mobile devices most likely do not make active connection to a telecommunications network when they are left at home or at the office, as they will most likely be actively connected to a private network.

Furthermore, the European Court of Justice has considered it instructive to consider whether the collection and storage of data can cause the individuals concerned "to feel that their private lives are the subject of constant surveillance".[670] The media has reported that individuals have already reached out to their providers and the Autoriteit Persoonsgegevens, the Dutch data protection authority, to express their concerns and dissent.[671] Furthermore, the five-step scheme could result in the proactive implementation or reintroduction of control measures at the national, regional or local level.[672] This could certainly affect the fundamental right to privacy in the sense that it could have a significant impact on an individual's private life.[673]

Third, the Dutch government seeks to build on the current business practice of collecting and storing traffic and location data for a limited time for purposes of accurately billing end-users.[674] However, the proposed temporary act compels telecommunications providers to perform new processing operations, which require a legal basis that the proposed temporary act would establish. The telecommunications providers would need to store traffic and location data onto dedicated network systems, use traffic and location data to determine a mobile device's hourly locations, storage, and use hourly locations to determine a mobile device's municipality of origin, use hourly locations and municipality of origin to infer mobility data, and transmit mobility data to the CBS. Considering those processing operations, one can argue that in contrast to the Dutch government's stance,[675] the proposed temporary act actually imposes a (general and indiscriminate) data retention obligation on telecommunications providers.

Fourth, the Dutch government incorrectly assumes that the mobility data received and processed by the CBS and the RIVM can be qualified as anonymous information.[676] According to recital 26 General Data Protection Regulation, anonymous information "does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable". To determine whether a natural person is identifiable, recital 26 General Data Protection Regulation clarifies that "account should be taken of all the means reasonably and likely to be used".[677] Even though space does not permit an extensive discussion of whether de-anonymization is "practically impossible",[678] we find it instructive to take into account the following four observations.

First, the notion "personal data" should be construed so broadly that it could cover any information,[679] whereas anonymity is a extremely hard to achieve because of a growing disconnect between legal theory and practical feasibility.[680] Research confirms that it is notoriously difficult to anonymise traffic and

[670] Compare *Tele2*, para 100; *Privacy International*, para 71.

[671] Jeroen Piersma en Martijn Pols, 'KPN weigerde locatiedata van klanten met Brussel te delen' *Het Financieele Dagblad* (Amsterdam, 30 June 2020) 12; Wilmer Heck, 'Privacywaakhond: spoedwet voor volgen van burgers via hun mobiele telefoon moet van tafel' *Nieuwe Rotterdamsche Courant* (Amsterdam, 3 July 2020) <https://www.nrc.nl/nieuws/2020/07/03/privacywaakhond-spoedwet-voor-volgen-van-burgers-via-hun-mobiele-telefoon-moet-van-tafel-a4004867> accessed 3 November 2020.

[672] See sections 1.2.4 and 1.2.5.

[673] Lotte Houwing, 'Schriftelijke inbreng Bits of Freedom. Tijdelijke wet informatieverstrekking RIVM i.v.m. COVID-19' (2020).

[674] *Parliamentary Papers II* 2019/20, 35479, nr. 2, 11.

[675] *Parliamentary Papers II* 2019/20, 35479, nr. 2, 11.

[676] *Parliamentary Papers II* 2020/21, 35479, nr. 10, 5 and 6.

[677] To determine whether a means is reasonably likely to be used to identify a natural person, "account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration [the state of the art] and technological developments". See recital 26 General Data Protection Regulation.

[678] With respect to the question whether a means is reasonably likely to be used to identify a natural person, the European Court of Justice held in *Breyer* stated "that would not be the case if the identification of the data subject was prohibited by law or practically impossible on account of the fact that it requires a disproportionate effort in terms of time, cost and man-power, so that the risk of identification appears in reality to be insignificant". See Case C-582/14 *Patrick Breyer v Bundesrepublik Deutschland* [2016] ECLI:EU:C:2016:779, para 46.

[679] Nadezhda Purtova, 'The law of everything. Broad concept of personal data and future of EU data protection law' (2018) 10(1) Law, Innovation and Technology 40.

[680] Michèle Finck, 'Blockchains and Data Protection in the European Union' (2018) 4(1) European Data Protection Law Review 17, 22-26; Michèle Finck and Frank Pallas, 'They who must not be identified—distinguishing personal from non-personal data under the GDPR' 2020 10(1) International Data Privacy Law 11; European Data Protection Board, 'Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak' (2020) 5 and 6.

location data from both a legal and technical perspective.[681] Furthermore, as long as telecommunications providers have the original traffic and location data stored on their general network systems for billing purposes, the risk of de-anonymization lingers.

Moreover, the Dutch government has not prohibited the CBS and the RIVM from de-anonymizing the data. While the Dutch government has bound the processing operations of the CBS and RIVM to the purpose of combatting infectious diseases, such a form of purpose limitation does not necessarily equate to a deanonymisation ban.[682] Additionally, the Dutch government has explained that the CBS and the RIVM can enrich mobility data by combining the data with other datasets,[683] which could result in the identification or the singling out of individuals, or at least make it easier to do so. Against that backdrop, it can even be argued that the proposed temporary act also imposes a (general and indiscriminate) data retention obligation on the CBS and the RIVM. Further, the European Court of Justice has explained that the transfer of traffic and location data to a third party—here: the CBS and the RIVM—already constitutes an interference with the principle of confidentiality, regardless of how the data is used, whether the data is sensitive, or whether the individuals concerned have been inconvenienced.[684]

What is more, there is a chance that nefarious entities will be able to appropriate mobility data and de-anonymize it for malicious ends. While European telecommunications providers been subject to cybersecurity attacks,[685] the media has reported a data breach at the RIVM, which indicates that at least some of the Dutch institution’s technical measures are inadequate.[686] According to the Court, when a generic data retention measure provides for the continuous storage of vast amounts of sensitive traffic and location data, which seems to be the case for the proposed temporary act, the risk of abuse and unlawful access needs to be considered.[687]

All things considered, the proposed temporary act needs to be classified as a notably serious interference with fundamental rights due to its wide scope in combination with the low chance of successful data anonymisation and the potential threat of data breaches.

5.4.3 The general interests protected by the proposed temporary act: The pursuit of public security and public health

Article 15(1) ePrivacy Directive prescribes that any restriction needs to safeguard one of the following general interests: national security, defence, public security, or the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of an electronic communications system.

[681] Fengli Xu, Zhen Tu, Yong Li, Pengyu Zhang, Xiaoming Fu and Depeng Jin, ‘Trajectory Recovery From Ash: User Privacy Is NOT Preserved in Aggregated Mobility Data’ (International Conference on World Wide Web, Perth, April 2017); Vagelis Papakonstantinou and Paul de Hert, ‘Big data analytics in electronic communications: A reality in need of granular regulation (even if this includes an interim period of no regulation at all)’ (2020) 36 Computer Law and Security Review 1, 8-10; Letter from Matthijs Koot to Vaste commissie voor Economische Zaken en Klimaat (9 October 2020).

[682] Article 14.7(1) Dutch Telecommunications Act in conjunction with Article 6 Wet publieke gezondheid; *Parliamentary Papers II* 2020/21, 35479, nr. 10, 1 and 2.

[683] *Parliamentary Papers II* 2019/20, 35479, nr. 2, 4; *Parliamentary Papers II* 2019/20, 35479, nr. 7, 11, 22 and 26.

[684] *Privacy International*, paras 70 and 72.

[685] European Union Agency for Cybersecurity, ‘Telecom Services Security Incidents 2019. Annual Analysis Report’ (2020) 18; Melinda Rucz and Sam Kloosterboer, ‘Data Retention Revisited’ (2020) 21 and 22.

[686] Joost Schellevis, ‘Lek in RIVM-Coronasite: gegevens van gebruikers makkelijk in te zien’ (*NOS*, 6 June 2020) <https://nos.nl/artikel/2336416-lek-in-rivm-Coronasite-gegevens-van-gebruikers-makkelijk-in-te-zien.html> accessed 9 November 2020; ‘Geen misbruik datalek Infectieradar’ (*RIVM*, 8 June 2020) <https://www.rivm.nl/nieuws/geen-misbruik-datalek-infectieradar> accessed 9 November 2020.

[687] Compare *Privacy International*, para 73; *La Quadrature du Net*, para 119.

These general interests have to be interpreted in the same sense as former Article 13(1) Data Protection Directive[688] and current Article 23(1) General Data Protection Regulation.[689] Based on legislative documents, the Dutch government hopes to protect two general interests: public security within the meaning of Article 15(1) ePrivacy Directive; and public health, an important objective of general public interest, within the meaning of Article 23(1) General Data Protection Regulation.[690]

As a preliminary matter, it is important to take note of the following observations. First, the European Court of Justice has repeatedly stressed that the shortlist of general interests is exhaustive, meaning that Member States cannot adopt restrictions for purposes not listed in Article 15(1) ePrivacy Directive.[691] Second, the European Court of Justice has emphasized that the general interests being pursued need to correspond to the seriousness of the interference presented by the restriction: the more serious the interference is, the more serious the general interest should be.[692] Our conclusion that the proposed temporary act is a notably serious interference carries with it the notion that the proposed temporary act should safeguard a correspondingly serious general interest. Third, the European Court of Justice has recently identified a hierarchy within the enumeration: the protection of national security can justify the most serious of interferences, whereas the enforcement of ordinary and serious crimes, as well as the protection of public security, can never justify such serious interferences.[693]

Regarding public security, the question is whether the Dutch government can argue successfully that the proposed temporary act would protect the general interest. Because the Court has not provided much interpretative guidance within the context of Article 15(1) ePrivacy Directive, considering case law on public security within the meaning of the Treaty of the Functioning of the European Union[694] could be instructive.[695] Within that context, the European Court of Justice has underscored that while Member States have the freedom to determine the requirements of public security, the European Union continues to exercise control over their scope.[696] Furthermore, the European Court of Justice has declaredan internal as well as an external dimension to public security. Direct threats to the functioning of institutions and essential public services, as well as the peace of mind and physical security of a Member State's population, concern the internal dimension. Risks of the serious disturbance of a Member State's foreign relations as well as a nation's peaceful coexistence concern the external dimension.[697] Considering these precedents, which leave Member States a margin of appreciation in combination with the pandemic's profound impact, the Dutch government could potentially argue successfully that eliminating the Corona virus is indeed a matter of public security. In other words, the pandemic has mutated into a threat to public security.[698]

[688] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/31.

[689] Article 15(1) ePrivacy Directive. The ePrivacy Directive refers to the Data Protection Directive and not to the General Data Protection Regulation. Since 25 May 2018, the Data Protection Directive has been repealed and replaced by the General Data Protection Regulation, making any reference to the Data Protection Directive seen as a reference to the General Data Protection Regulation. See Articles 94(1) and 99(2) General Data Protection Regulation. Consequently, Article 15(1) ePrivacy Directive should now be read as referring to Article 23(1) General Data Protection Regulation, which largely reproduces Article 13(1) Data Protection Directive. See Article 94(2) General Data Protection Regulation; Case C-673/17 *Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband eV v Planet49 GmbH* [2019] ECLI:EU:C:2019:801, para 38-42.

[690] *Parliamentary Papers II* 2019/20, 35479, nr. 2, 5.

[691] *Tele2*, paras 90 and 115; *Ministerio Fiscal*, para 52; *La Quadrature du Net*, para 112.

[692] *Tele2*, para 102; *Ministerio Fiscal*, paras 53-63; *Privacy International*, paras 67 and 75; *La Quadrature du Net*, paras 130, 131 and 145-147.

[693] *Privacy International*, paras 74 and 75; *La Quadrature du Net*, paras 134-136.

[694] Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union [2012] OJ C326/1.

[695] We do not research whether public security also covers fighting a pandemic further because of the margin of appreciation that the Member States enjoy under European Union law.

[696] See e.g. Joined Cases C-331/16 and C-366/16 *K. v Staatssecretaris van Veiligheid en Justitie and H. F. v Belgische Staat* [2018] ECLI:EU:C:2018:296, para 40.

[697] See e.g. Case C-145/09 *Land Baden-Württemberg v Panagiotis Tsakouridis* [2010] ECLI:EU:C:2010:708, para 44; Case C-601/15 PPU *J. N. v Staatssecretaris voor Veiligheid en Justitie* [2016] ECLI:EU:C:2016:84, para 66; Joined Cases C-331/16 and C-366/16 *K. v Staatssecretaris van Veiligheid en Justitie and H. F. v Belgische Staat* [2018] ECLI:EU:C:2018:296, para 42.

[698] Compare Hannah van Kolfschooten and Anniek de Ruijter, 'COVID-19 and privacy in the European Union: A legal perspective on contact tracing' (2020) 41(3) 478, 479. More generally, see Hylke Dijkstra and Anniek de Ruijter, 'The Health-Security Nexus and the European Union: Toward a Research Agenda' (2017) 8(4) European Journal of Risk Regulation 613.

Regarding public health, the question is whether the Dutch government can actually rely on the general interest to adopt the proposed temporary act. Even though public health is not expressly listed in Article 15(1) ePrivacy Directive, the European Court of Justice has established a bypass in *Promusicae*, which the government could invoke in order to adopt the proposed temporary act for such objectives. In *Promusicae*, the court argued that a cross-reference to Article 13(1) Data Protection Directive in Article 15(1) ePrivacy Directive implies that Member States can adopt restrictions necessary for the protection of the public's rights and freedoms.[699] In *Tele2*, the court took things one step further, deciding that Member States can adopt restrictions to protect any general interest in Article 13(1) Data Protection Directive.[700] These rulings open the door to adopting the proposed temporary act for public health objectives.

Even though this expansive interpretation of the shortlist was later reaffirmed in *LSG*[701] and *Bonnier Audio,*[702] certain arguments negate the court's precedents. First, the formulation of Article 15(1) ePrivacy Directive, "as referred to" emphasizes that the enumeration of general interests should actually be interpreted restrictively.[703] The more so because the European legislature has only transposed a selection of the general interests in Article 13(1) Data Protection Directive into Article 15(1) ePrivacy Directive.[704] Second, an expansive interpretation is hard to reconcile with the proviso that any derogation from or limitation of fundamental rights to privacy and data protection is only permitted to the extent that it is strictly necessary.[705]

Against the backdrop of these counterarguments, the Dutch government should not be able to call on public health to adopt the proposed temporary act. Nonetheless, the pandemic could call for a more balanced approach towards Article 15(1) ePrivacy Directive, potentially justifying an expansive interpretation that would legitimise adopting the proposed temporary act for public health objectives. The crux of the matter is that we do not know how the European Court of Justice would rule on this instance. What we do know is that caution should be exercised as much as possible in order to not give Member States the impression that they can operationalise surveillance schemes for considerably more general interests than expressly listed in Article 15(1) ePrivacy Directive. The Dutch government seems to be in the fortunate position that it can mute the foregoing discussion by arguing that the proposed temporary act would only protect public security.

5.4.4 The necessity of the proposed temporary act

Article 15(1) ePrivacy Directive dictates that any restriction needs to be a necessary, appropriate and proportionate measure within democratic society.[706] Recital 11 ePrivacy Directive specifies that any restriction must be strictly proportionate to its intended purpose.[707] This final condition is a high bar to clear.

[699] Case C-275/06 *Productores de Música de España (Promusicae) v Telefónica de España SAU* [2008] ECLI:EU:C:2008:54, paras 52-54.

[700] *Tele2*, § 90 and 115.

[701] Case C-557/07 *LSG-Gesellschaft zur Wahrnehmung von Leistungsschutzrechten GmbH v Tele2 Telecommunication GmbH* [2009] ECLI:EU:C:2009:107, paras 26 and 27.

[702] Case C-461/10 *Bonnier Audio AB, Earbooks AB, Norstedts Förlagsgrupp AB, Piratförlaget AB, Storyside AB v Perfect Communication Sweden AB* [2012] ECLI:EU:C:2012:219, para 55.

[703] Case C-275/06 *Productores de Música de España (Promusicae) v Telefónica de España SAU* [2008] ECLI:EU:C:2008:54, Opinion of AG Kokott, paras 86 and 87.

[704] Case C-275/06 *Productores de Música de España (Promusicae) v Telefónica de España SAU* [2008] ECLI:EU:C:2008:54, Opinion of AG Kokott, paras 86 and 87; Wilfred Steenbruggen, *Publieke dimensies van privé-communicatie: een onderzoek naar de verantwoordelijkheid van de overheid bij de bescherming van vertrouwelijke communicatie in het digitale tijdperk* (Otto Cramwinckel Uitgever 2009) 179-186; W. Steenbruggen, 'COVID-19 en de e-Privacyverordening: nog meer hoofdpijn?' (2020) 4 Computerrecht 219, 220.

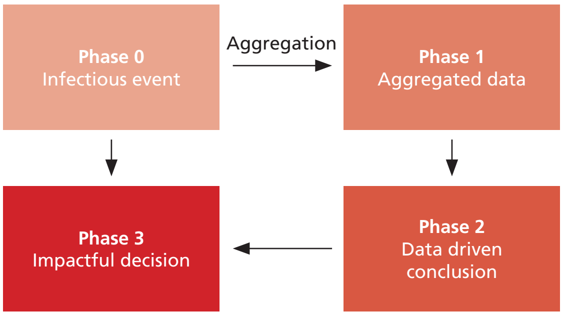
[705] Case C-73/07 *Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy, Satamedia Oy* [2008] ECLI:EU:C:2008:727, para 56; Joined Cases C-92/09 and C-93/09 Volker und Markus Schecke GbR, Hartmut Eifert v Land Hessen [2010] ECLI:EU:C:2010:662, paras 77 and 86; Case C-473/12 *Institut professionnel des agents immobiliers (IPI) v Geoffrey Englebert, Immo 9 SPRL, Grégory Francotte* [2013] ECLI:EU:C:2013:715, para 39; *Digital Rights Ireland*, para 52; Case C-212/13 *František Ryneš v Úř ad pro ochranu osobních údajř* [2014] ECLI:EU:C:2014:2428, para 28; *Tele2*, para 96; Opinion 1/15 [2017] ECLI:EU:C:2017:592, para 140; Case C-73/16 *Peter Puškár v Finanř né riaditeř stvo Slovenskej republiky, Kriminálny úrad finanř nej správy* [2017] ECLI:EU:C:2017:725, paras 38 and 112, *Privacy International*, para 67; *La Quadrature du Net*, para 130.

[706] Article 15(1) ePrivacy Directive.

[707] *Tele2*, para 95; *Privacy International*, paras 66 and 67; *La Quadrature du Net*, paras 129 and 130.

The proposed temporary act would introduce a four-step scheme with two objectives. First, it would enable the RIVM to continuously assess the effectiveness of the containment and mitigation measures in force.[708] Second, it would enable the RIVM to proactively inform national, regional, and local authorities about the possible resurgence of the Corona virus, which could result in the implementation or reintroduction of containment and mitigation measures at the national, regional, or local level.[709] Even though research concludes that mobility can be an appropriate means in the elimination of the Corona virus,[710] the Dutch government has failed to explain which distinctive features set the proposed temporary act apart from other solutions, which in combination with the impact on fundamental rights, as well as a lack of adequate safeguards, suggests the proposed temporary act cannot be considered a necessary and proportionate measure within democratic society under Article 15(1) ePrivacy Directive. We plead our case by discussing the following visual.

Figure 3. 4-step workflow under the proposal



The Dutch government has stated that the four-step scheme could be used to determine the mixing of residents from different municipalities. Those findings could be used by the RIVM to predict how the Corona virus would spread across the country and to inform especially regional and local authorities about regional and local trends.[711] The Dutch government has used the following scenario to explain its statement. Suppose that many Bergen op Zoom residents visit Roosendaal on a Saturday, that many Roosendaal residents test positive for the Corona virus the following week, and that mobility data shows no notable deviations in intermunicipal movement other than between Bergen op Zoom and Roosendaal.[712] According to the Dutch government, the RIVM should be able to proactively inform the authorities in Bergen op Zoom that residents might have an increased risk of contracting the Corona virus.[713] Subsequently, the local authorities in Bergen op Zoom would be able to take local containment and mitigation measures, such as targeted contact tracing in order to uncover visits to Roosendaal as a possible cause of infection.[714] We understand this to be the Dutch government's conception of the added value of the proposed temporary act.

[708] Article 14.7(1) Dutch Telecommunications Act; *Parliamentary Papers II* 2019/20, 35479, nr. 2, 3 and 4; *Parliamentary Papers II* 2019/20, 35479, nr. 7, 14.

[709] Article 14.7(1) Proposal; *Parliamentary Papers II* 2019/20, 35479, nr. 2, 3 and 4; *Parliamentary Papers II* 2019/20, 35479, nr. 7, 14.

[710] See e.g. Caroline O. Buckeel, Satchit Balsari, Jennifer Chan, Mercè Crosas, Francesca Dominici, Urs Gasser, Yonatan H. Grad, Bryan Grenfell, M. Elizabeth Halloran, Moritz U. G. Kraemer, Marc Lipsitch, C. Jessica E. Metcalf, Lauren Ancel Meyers1, T. Alex Perkins, Mauricio Santillana, Samuel V. Scarpino, Cecile Viboud, Amy Wesolowski, Andrew Schroeder, 'Aggregated mobility data could help fight COVID-19' (2020) 368(6487) Science 145; Nuria Oliver, Bruno Lepri, Harald Sterly, Renaud Lambiotte, Sébastien Deletaille, Marco De Nadai, Emmanuel Letouzé, Albert Ali Salah, Richard Benjamins, Ciro Cattuto, Vittoria Colizza, Nicolas de Cordes, Samuel P. Fraiberger, Till Koebe, Sune Lehmann, Juan Murillo, Alex Pentland, Phuong N Pham, Frédéric Pivetta, Jari Saramäki, Samuel V. Scarpino, Michele Tizzoni, Stefaan Verhulst, Patrick Vinck, 'Mobile phone data for informing public health actions across the COVID-19 pandemic life cycle' (2020) 6(23) Science Advances 1.

[711] *Parliamentary Papers II* 2019/20, 35479, nr. 2, 3.

[712] *Parliamentary Papers II* 2019/20, 35479, nr. 2, 3.

[713] *Parliamentary Papers II* 2019/20, 35479, nr. 2, 3.

[714] *Parliamentary Papers II* 2019/20, 35479, nr. 2, 3; *Parliamentary Papers II* 2019/20, 35479, nr. 7, 18.

However, the government has omitted important information from this scenario: the actual event that the mobility data should identify. Why did many residents of Bergen op Zoom visit Roosendaal on Saturday? Would this event have gone unnoticed had the RIVM not had access to mobility data? The government seems to have answered the latter question in the affirmative. But over the course of the pandemic, regional and local authorities have shown themselves to be well-aware of regional and local events causing notable intermunicipal movement, which could be attributed to information such as permit applications and real-time observations. Also, regional and local authorities have shown they are already be well-equipped to take proactive and real time containment and mitigation actions on a regional and local level. The Dutch government seems to have reinforced this point by noting that follow-on action under the proposed temporary act would be determined predominantly by local authorities.[715] As a result, we would answer the above question in the negative, which suggests that regional and local authorities would not necessarily need the five-step mechanism to detect notable intermunicipal movements and take action.[716]

Furthermore, even though the double aggregation of mobility data could contribute to preserving end-user privacy, it makes mobility data less granular and robust. First, telecommunications providers need to discard any total number fewer than 15 mobile devices from mobility data.[717] Second, the CBS must round the consolidated mobility data to the nearest 50 mobile devices.[718] This defeats most hope of seeing any notable deviations in intermunicipal movement between small municipalities. Suppose that in one hour KPN registers 24 residents of Terschelling as visiting Waadhoeke, and that Vodafone and T-Mobile both register 14 other residents paying the same visit. The mobility data would report on intermunicipal movement as zero, even though 52 residents of Terschelling visited Waadhoeke. Now suppose that during another hour KPN registers 74 residents of Terschelling visiting Waadhoeke, and that Vodafone and T-Mobile both register 14 other residents paying the same visit. The mobility data would report the intermunicpal movement as 50, even though 102 residents from Terschelling visited Waadhoeke. As intermunicipal movement between larger municipalities tends to be consistently large and municipalities seem well-aware of events causing notable intermunicipal movement, we expect that the added value of the proposed temporary act would be found in charting unusual intermunicipal movement between smaller municipalities, such as Terschelling and Waadhoek. But the five-step mechanism does not seem designed to meaningfully report on such movements.

Moreover, the proposed temporary act's underwhelming added value does not seem to counterbalance the notable seriousness of the inference presented to fundamental rights. The RIVM cannot use mobility data to determine the actual mixing of infected residents of Roosendaal and non-infected residents of Bergen op Zoom. Rather, the RIVM can only use mobility data to estimate the potential risk of virus transmission between individuals.[719] This is an important distinction. The more so because the Netherlands already has a contract tracing network in place for ascertaining the degree of proximity between infected and non-infected individuals. What more is the proposed temporary act going to add? The added value seems to lay in the creation of statistical models that could predict how the Corona virus would spread across the country.[720]

All things considered, could the Dutch government argue convincingly that the added value of the proposed temporary act is proportionate to the notable seriousness of the interference with fundamental rights? This question seems to be one that the Dutch government struggles with. Having been repeatedly

[715] *Parliamentary Papers II* 2019/20, 35479, nr. 7, 11, 17 and 28.

[716] Sarah Eskens and Jurriaan van Mil, 'Doorsturen telecomdata naar RIVM vereist een beter verhaal' *Het Financieele Dagblad* (Amsterdam, 12 September 2020) 39.

[717] Article 14.7(5) Dutch Telecommunications Act.

[718] *Parliamentary Papers II* 2020/21, 35479, nr. 10, 5.

[719] *Parliamentary Papers II* 2019/20, 35479, nr. 2, 4.

[720] Sarah Eskens and Jurriaan van Mil, 'Doorsturen telecomdata naar RIVM vereist een beter verhaal' *Het Financieele Dagblad* (Amsterdam, 12 September 2020) 39.

asked, it has inadvertently admitted it does not know: "The point is that, precisely because [mobility data] is currently not available, it is not possible to indicate how [such data] could have been a necessary complement in an existing situation."[721] Put differently, the proposed temporary act's added value is underwhelming at best and non-existent at worst. How can the proposed temporary act then be considered a necessary and proportionate measure within democratic society, especially considering the impact on fundamental rights? Even though we have focussed on the Dutch situation, our considerations and observations apply (*mutatis mutandis*) to supranational and foreign initiatives. What do other countries hope to deduce from telecommunications data and for what purposes do they intend to use their findings? Would it be possible to use less intrusive solutions to achieve the same, or at least a similar, outcome?

Furthermore, the proposed temporary act does not include adequate legal safeguards to overturn the above conclusion.[722] Considering the legal safeguards prescribed by the European Court of Justice within the context of data retention and access legislation is instructive because there are notable similarities between such legislation and the proposed temporary act. The presence of such legal safeguards should not immediately make the proposed temporary act a proportionate and necessary measure within democratic society as long as the Dutch government remains undecided on what the proposed temporary act should add to its already large Corona virus toolbox.

First, the European Court of Justice has prescribed that a legislative measure needs to include clear and precise rules on the scope and application of the data retention obligation, which needs to indicate in which circumstances and under which conditions such an obligation can be imposed.[723] Such information is missing in the proposed temporary act. Some its criteria and parameters are unclear or undefined, though some clarification can be expected when it has been adopted.[724] Do the Minister of Economic Affairs and the Minister of Health need to consider any circumstances, such as the severity of the threat presented by the Corona virus, and conditions, such as the informed recommendation of academics, before instructing telecommunications providers to share mobility data with the CBS? How is the RIVM going to ensure that authorities cannot distinguishmobility data, and possibly personal data, from its notification, especially when reporting on smaller municipalities? Considering the proposed temporary act's notably serious impact on fundamental rights, the foregoing information should have been included in the proposed temporary act in order to provide some consolation. Moreover, such omissions make it difficult to ascertain and appraise the extent to which the proposed temporary act is legally, logically, and technically sound. Such omissions, whether conscious or not, run contrary to the European Court of Justice's case law.

Second, the European Court of Justice ruled in *Tele2* that data access legislation needs to be subject to *ex ante* review by a court or an independent administrative body at the reasoned request of a competent national authority.[725] However, the legislative proposal does not prescribe that the Minister of Economic Affairs and Minister of Health seek the authorisation of a court or an independent administrative body before instructing telecommunications providers to share mobility data with the CBS.

Third, the European Court of Justice held in *Tele2* that telecommunications providers need to take appropriate technical and organisational measures to ensure that their level of protection and security corresponds to the seriousness of an interference.[726] Such cybersecurity measures include storing data within

[721] *Parliamentary Papers II* 2019/20, 35479, nr. 7, 28.

[722] Sarah Eskens and Jurriaan van Mil, 'Doorsturen telecomdata naar RIVM vereist een beter verhaal' *Het Financieele Dagblad* (Amsterdam, 12 September 2020) 39.

[723] *Tele2*, para 109, *Privacy International*, para 68; *La Quadrature du Net*, para 132.

[724] Article 14.7(6) Proposal; *Parliamentary Papers II* 2019/20, 35479, nr. 3, 4.

[725] Joined Cases C-203/15 and C-698/15 *Tele2 Sverige AB v Post-och telestyrelsen, and Secretary of State for the Home Department v Tom Watson, Peter Brice, Geoffrey Lewis* [2016] ECLI:EU:C:2016:970, para 120.

[726] Joined Cases C-203/15 and C-698/15 *Tele2 Sverige AB v Post-och telestyrelsen, and Secretary of State for the Home Department v Tom Watson, Peter Brice, Geoffrey Lewis* [2016] ECLI:EU:C:2016:970, para 122.

the European Union and irreversibly destructing data once the retention period has elapsed.[727] The proposed temporary act's notably serious impact on fundamental rights implies that the Dutch government should incorporate in the proposed temporary act that telecommunications providers, the CBS, and the RIVM need to provide an appropriate level of protection and security, even when they are not already subject to other cybersecurity obligations.

Fourth, the European Court of Justice ruled in *Tele2* that Member States need to ensure that data access legislation is subject to *ex post* review by an independent authority.[728] The Dutch government has stated that the Autoriteit Persoonsgegevens and the Agentschap Telecom will oversee whether telecommunications providers comply with the proposed temporary act pursuant to the Dutch Telecommunications Act.[729] This would mean that the regulatory authorities cannot exercise jurisdiction over the CBS and the RIVM.[730] The more so because of the Dutch government's departure from the premise that the CBS and RIVM process anonymous information rather than personal data.[731] This would mean that their data processing operations are neither governed by the General Data Protection Regulation nor overseen by the Autoriteit Persoonsgegevens.[732] Whether this contentious premise is correct or not, the Dutch government would be well advised to extend the Autoriteit Persoonsgegevens' and the Agentschap Telecom's mandate on purpose to cover supervising the CBS's and RIVM's processing operations pursuant to the proposed temporary act.[733] The lack of the above legal safeguards adds to our conclusion that the proposed temporary act cannot be considered a necessary and proportionate measure within a democratic society.

5.5 Conclusion

All things considered, we conclude that the legislature is not in accordance with the principle of confidentiality introduced by the ePrivacy Directive and implemented in the Dutch Telecommunications Act. Even though we applaud the Dutch government for involving the Parliament rather than having telecommunications providers simply share presumed anonymous mobility data, the proposed temporary act falls short: it does not add much to the Dutch government's Corona virus toolbox and is not subject to adequate legal safeguards,[734] making that it cannot meet the considerably high standards set by the Article 15(1) ePrivacy Directive. Adopting the proposed temporary act would force telecommunications providers to systematically breach the principle of confidentiality, thereby having a serious impact on fundamental rights. Our research informs the debate on the proposed temporary act in case the Dutch government reboots the legislative procedure, demonstrating that the ePrivacy Directive defines the limits of what Member States can lawfully do with telecommunications data in a robust manner. Furthermore, our research informs the public debate elsewhere because our considerations and observations pertaining to the questions "What should using telecommunications data achieve and can that be achieved using less intrusive means?" are relevant across the globe.

Considering the European Commission's push for using telecommunications data in the eradication of the Corona virus, we would not be surprised when the Dutch government drops the proposed temporary act

[727] Joined Cases C-203/15 and C-698/15 *Tele2 Sverige AB v Post-och telestyrelsen, and Secretary of State for the Home Department v Tom Watson, Peter Brice, Geoffrey Lewis* [2016] ECLI:EU:C:2016:970, para 122.

[728] Joined Cases C-203/15 and C-698/15 *Tele2 Sverige AB v Post-och telestyrelsen, and Secretary of State for the Home Department v Tom Watson, Peter Brice, Geoffrey Lewis* [2016] ECLI:EU:C:2016:970, para 123.

[729] *Parliamentary Papers II* 2019/20, 35479, nr. 2, 21.

[730] *Parliamentary Papers II* 2019/20, 35479, nr. 2, 21.

[731] *Parliamentary Papers II* 2020/21, 35479, nr. 10, 5 and 6.

[732] *Parliamentary Papers II* 2020/21, 35479, nr. 10, 5 and 6.

[733] For a discussion of how oversight could be designed, see Sarah Eskens, Ot van Daalen and Nico van Eijk, '10 Standards for Oversight and Transparency of National Intelligence Services' (2016) 8(3) Journal of National Security Law & Policy 553.

[734] Sarah Eskens and Jurriaan van Mil, 'Doorsturen telecomdata naar RIVM vereist een beter verhaal' *Het Financieel Dagblad* (Amsterdam, 12 September 2020) 39.

in favour of informal cooperation between the various relevant parties, as we are seeing in other Member States such as France. But this would not mean the Dutch government will resolve the underlying issues identified by our research.

More fundamentally, this instance of jumping to telecommunications data to battle against the Corona virus lays bare the normative question: how desirable is the operationalisation of intrusive technological solutions under time pressure as a result of a crisis such as the COVID-19 crisis from a fundamental rights perspective? Rather than immediately championing a far-reaching collection of data in the name of public security or public health, should we not pay more attention to the risk of normalisation once the crisis is over?

6 Expert opinion: Considering the ethical issues of invasive technologies Data Ethics Decision Aid (DEDA) & CoronaMelder

Expert opinion by David van den Berg, junior researcher, Utrecht Data School, Utrecht University, Lisa de Graaf, Project Manager DataWerkplaats, Utrecht Data School, Utrecht University & Mirko Tobias Schäfer, Associate Professor, Project Lead, Utrecht Data School, Utrecht University, University of Utrecht, Utrecht Data School[735]

6.1 Setting the scene: the *CoronaMelder* app

During the press conference on 7 April 2020, Hugo de Jonge, Dutch Minister of Health, Welfare, and Sport, announced the introduction of a Corona app for tracing infections and mitigating the risks of the disease's spread (hereafter: the app). Most importantly, the app was heralded as the "intelligent exit" of the so-called intelligent lockdown. The app was considered a great aid in flattening the curve, yet there was little to no guidance for app developers to follow. Other countries had already introduced similar solutions, though research at the time indicated that all other apps for tracing COVID-19 contamination were ineffective, in part because they created a false sense of security (Sweeney, 2020). They also constituted a significant likelihood for infringing upon fundamental rights (Coghlan, Cheong, & Coghlan, 2020). While there was no proof that these apps were actually effective in tracing COVID contamination, they raised concerns about possible infringement on fundamental rights. In the Netherlands, experts from different fields quickly responded with criticism towards the vague plans and the lack of clear objectives, premises, and boundaries for such invasive technology.[736] However, the government still made a call for proposals,[737] though it provided no concrete purpose for the app, nor minimal requirements for it. The only guideline given was that all proposals should respect privacy and be secure. In a public "appathon" streamed on YouTube, the Dutch government tried to establish a more transparent process for screening seven app proposals that had been arbitrarily selected from 660 entries. These proposals were broad, and some went beyond the initial idea of the app, namely the tracing and tracking of COVID-19 infections. Others disregarded some of the basic requirements, such as data minimization, transparency or privacy. The latter was the main focus of most proposals, yet there were more glaring issues. Core values such as freedom, trust, personal rights and reliability were at risk with the hastened implementation of the Corona app, besides the more "obvious" values such as privacy and security. While many of the proposals were dismissed due to pronounced security issues and design flaws, it became clear that invasive technologies used for crisis response required a thorough review process. This process must consider the broader societal impact, define boundaries, and be based on clearly defined objectives and proven effectiveness.

[735] Utrecht Data School is a platform for teaching data analysis and digital methods, and for investigating the impact of datafication and algorithmisation on citizenship and democracy. www.dataschool.nl

[736] See this letter to the government strongly advising against the hasty implementation of tracking technology and warning of possible infringement on fundamental rights. The letter was signed by over 60 scientists and scholars from the fields of computer science, law, ethics, media, political sciences and others. <http://allai.nl/wp-content/uploads/2020/04/Brief-Minister-President-Rutte-Ministers-De-Jonge-Van-Rijn-Grapperhaus-de-heer-Sijbesma-inzake-COVID-19-tracking-en-tracing-en-gezondheidsapps.pdf>; or the Veilig tegen Corona [Safely against Corona] initiated by advocacy groups Bits of Freedom, Amnesty International, De Waag Society and others: <https://www.veiligtegenCorona.nl/>

[737] See the tender for a software solution for tracing Corona infections, as advertised by the Ministry for Health, Welfare & Sport: <https://www.tenderned.nl/tenderned-tap/aankondigingen/192421>

This expert opinion introduces the Data Ethics Decision Aid (DEDA) as a feasible tool in facilitating an evaluation of technologies such as the *CoronaMelder* app for their societal impact.

6.2 A brief note on terminology

The field of ethics of technology is full of ambiguous terminology. This ambiguity is visible on (amongst others) a philosophical-theoretical level, with authors making distinctions between information ethics, digital ethics, (big) data ethics, and more (e.g., Floridi, 2010; Floridi, Cath, & Taddeo, 2018; Zwitter, 2014). This report does not engage with current conceptual debates, nor does it discuss data ethics in-depth. The choice of data ethics and related concepts are of a pragmatic nature. The same goes for concepts like digitization and data projects. The Data Ethics Decision Aid (DEDA) facilitates ethical reflection on all types of projects involving data and is not limited to data projects that use algorithms (decision trees, rule-based algorithms, machine learning, or otherwise). Therefore, we use the term data projects as interchangeable with similar terms.

6.3 Data Ethics Decision Aid (DEDA)

The Data Ethics Decision Aid (DEDA) is a framework used for the ethical impact assessments of data projects (Franzke, Muis, Schäfer, 2021). A dialogical process, DEDA brings together the various participants and stakeholders of a data project and enables them to revisit the data project, and its impact and consequences from different perspectives.[738] The topics and questions of DEDA guide the project team in their decision-making process, whilst also making sure the basic requirements and objectives of a project are clearly stated and argued. DEDA makes values explicit and indicates how a project's specific design decisions will affect values. It identifies the values explicitly driving a data project—in the case of the *CoronaMelder,* privacy and security. As such, DEDA encourages revisiting data projects not merely from a set of general core values, but rather from how values are affected by the project, focusing on consequences and responsibilities. It would question how the design actually represents the values of privacy and security, and whether those are transformed or affect other values (e.g., non-discrimination, trust, equality, autonomy, etc.). While the *CoronaMelder* eventually complied with some of the requirements formulated by critics, a recent analysis points to shortcomings of the app.[739] Many of the highlighted issues would have been addressed in a DEDA review process.

For this report, we will briefly summarize how DEDA works, outline the requirements for an effective DEDA review process, and discuss the (potential) results. This is not an exhaustive description of DEDA, but merely serves to illustrate the practical side of the framework. Finally, we will look at the *CoronaMelder* app and examine it in light of the DEDA requirements and potential results.

6.4 How-to DEDA

Considering the case of a data project, the Data Ethics Decision Aid facilitates a deliberative review process among a group of participants directly working on the project or who are relevant for it. The many guidelines and manifestos for AI and data ethics consist of underlying political, social and economic goals[740]. They (mostly) present normative values that should be taken into account when developing data projects. In comparison, DEDA is a rather "empty" tool that allows users to input their own values, or in the case

[738] Utrecht Data School, Data Ethics Decision Aid: <www.dataschool.nl/en/deda>
[739] Amnesty et al. 2020: <https://www.veiligtegencorona.nl/toetsing-veiligtegencorona-criteria.pdf>
[740] Algorithm Watch, global inventory: <https://inventory.algorithmwatch.org/about>

of a government organisation, public values. Additionally, they can consider relevant related jurisdiction and jurisprudence to make their argument for or against certain decisions concerning the data project, which is facilitated through questions on a broad range of topics. The questions are often deliberately open to encourage brainstorming about possible harms or undesired consequences and to provoke participants to come up with solutions for safeguarding the values and demographics of those who might be affected. DEDA emphatically focuses on the context in which a data project is implemented. It provides direct assistance in the development of a responsible data project process rather than merely delivering a framework that meets ethical requirements on paper. Documenting the reflections on values and design, and how the decision-making process unfolds, DEDA constitutes accountability. It enables critical audiences, the press, citizens, and political representatives to inspect how the process has been developed, which perspectives were considered along the way, which issues were flagged, and what decisions were taken in order to mitigate them.

Figure 4. DEDA in progress (pre-COVID-19)

6.5 DEDA requirements and (possible) results

Because the DEDA is an “empty” tool, its practical requirements need to be followed to achieve a good outcome. A good outcome here means a well-documented reflection and assessment of the affected values by the data project, and the concrete steps needed to safeguard them. Besides the obvious requirements of time and a decent project plan with a basic “what, how and why”, there are two further essential requirements that stand out.

Firstly, the DEDA requires the presence of relevant stakeholders and project participants. In order to guarantee a pluralistic value representation, the DEDA has to be done by a multidisciplinary team that includes (but is not limited to): a data scientist, domain expert, legal advisor, involved third-parties, political representative, etc. The second requirement is project-ownership. This means that the organization doing the assessment relies on individuals with enough authority to take the lead throughout the whole process, including a follow-up of the results. Using DEDA in numerous government organizations and companies, we found that the process exposes organisational shortcomings to fully accommodate data projects responsibly and effectively, such as operational capacities, organisational strategy, the definition of objectives, the definition of responsibilities, etc. (Siffels, van den Berg, Muis, Schäfer, forthcoming 2021). In order to benefit from insights and potentially close gaps, a high level of commitment is needed.

The results of the DEDA vary greatly from project to project and only reveal what the participants of the assessment contributed to it. When the above requirements have been met and the evaluation process has been carried out with sincere efforts to unearth ethical issues and create solutions to mitigate them, the DEDA results in concrete action points. These might address policy issues concerning the transparency of the data project, rules for procuring technology or services, and how to involve commercial stakeholders. At the same time, they might also be concrete points of action for the organisation to adapt their capacities, develop needed skills, issue communication strategies and make responsibilities explicit. These action points can vary in complexity and relevance. Some items might consider how data is visualized or who within the organisation should be kept in the loop; others might concern fundamental requirements for current and future data projects. As mentioned, the DEDA reveals gaps on various levels. An action point might indicate that the data project hasn't gone through an internal (or public) legitimacy process. Another point might reveal the lack of data infrastructure. This is why the requirement of DEDA-ownership is so fundamental. If an assessment reveals that there are problems with the development of the data project because there are gaps in (for example) the operational capacity of an organization, the authority to fix this rarely lies with the project leader of the said project. We cannot emphasize enough that data projects are not a mere technological issue that can be delegated to "data scientists", but very much an organisational, strategic and societal challenge that requires top management to consider diverse perspectives, as well as both short and long-term implications.

6.6 The *CoronaMelder* app & DEDA

When deploying potentially invasive technology as a crisis response, it is of utmost relevance to safeguard as many values as possible, as well as consider and exclude undesired side effects. It is necessary to make transparent whose interests are being served by developing and deploying the technology. As a thought experiment, it may be useful to try and forget the last 11 months and imagine a situation where a project team was tasked with the development of the *CoronaMelder* app. After the team put some basic ideas on paper, they decided to use the DEDA. Within this report, there is not enough space to do a full ethical assessment using DEDA; however, it is possible to use it as an outline for the issues that should be addressed, even if it momentarily leaves many design questions unanswered. Nevertheless, we have a general framework that facilitates ethical assessment. Using DEDA as a framework, it is not difficult to imagine what issues the project team may encounter. We think the project team would run into three main issues: a) stakeholder engagement b) requirements vs. abstract value, and c) explicating values. These main issues are intimately linked in practice but conceptually distinct.

6.7 Stakeholder engagement

As explained in the above requirements of the DEDA and argued for in the value-sensitive-design approach (Wynsberghe, Robbins, 2013), guaranteeing a pluralistic value representation is crucial in the development of responsible data projects. Since the beginning of the COVID-19 epidemic, and equally noticeable in the development of the *CoronaMelder* app, the voices around the decision table have been fairly homogeneous. The more individuals a data project affects, the more values are affected. Considering that the "winners" of the appathon were AI start-ups and large platform companies, it is unlikely that a broad spectrum of values were taken into account. The same goes for the experts judging the result, all experts in the fields of privacy, security, and health.[741] The experts involved already remarked on the hurried structure of the selection procedure, and other problems with the development process. However, there were no experts with knowledge about how to recognize and mitigate challenges for public values, which for

[741] Terugblik appathon, Rijksoverheid:
<https://www.rijksoverheid.nl/onderwerpen/Corona virus-app/tijdpad-proces-Corona virus-app/terublik-appathon>

instance, were raised by delegating an essential part of safeguarding public health to private companies without any sort of democratic legitimacy. Other concerns raised by the inclusion of parties like Google and Apple were also not considered.[742]

As these issues show, the development process insufficiently engaged with (responsible/relevant) stakeholders—a DEDA requirement. Yet, in the narrative surrounding the appathon, it was presented as being open, transparent and engaging the public. An open process is not the same as one considered democratic. An open process does not guarantee a pluralistic value approach, nor does it legitimize it. Stakeholder engagement does not equate more with better, but ought to be about the inclusion of relevant stakeholders with relevant values. For the app, we could consider how communication advisors, ethicists, general practitioners, social scientists, etc. would be relevant stakeholders. In order to represent their values in the development of the app, they need to be involved from the beginning of the development, not merely as judges after the fact.

6.8 Requirements vs abstract goals

One of the first questions of the DEDA addresses the objectives of the proposed projects. For the development of the *CoronaMelder* app, no clear goals were defined. It was presented as an easy solution to a complex problem without any evidence that the proposed app could serve this objective effectively. The Dutch government's rhetoric surrounding the app was a display of 'techno-solutionism' (see Morozov 2013:5). Such rhetoric evades considering proven effectiveness and defining requirements and boundaries for the app. DEDA makes that explicit by addressing the objectives and potential ethical issues. The invitation for the appathon vaguely called for 'smart digital solutions'.[743] Additionally, it expressed the need for security and privacy multiple times. Focusing merely on security and privacy overshadowed any consideration of other fundamental rights or values that might be affected. This lack of clearly defined objectives grounded in proven effectiveness and based upon robust legitimacy was noted by experts judging the appathon in the media.[744] When using the DEDA as a framework to examine the app, the lack of concrete goals leads to (at least) two related issues.

First, in order to complete an ethical assessment, a data project has to be clearly defined and delineated. This is why a (good) project plan is a fundamental requirement for using the DEDA. If the project team is unable to answer basic questions related to the goal of the project, who it affects, which data is being used, etc., they will also be unable to answer the specific questions that will help them develop a responsible data project. To make this even more tangible, take the example of anonymization/pseudonymization and access. Without a clear goal in mind, the project team is unable to decide which data needs to be pseudonymized and who has/needs the authority to reverse said pseudonymization. This creates a legal issue due to GDPR requirements, but also ethical issues regarding responsibility and accountability.

The second issue that the DEDA makes visible when the project goal is not clearly defined concerns the action points ethical assessments lead to. When the DEDA requirements are met and the assessment is completed, a project team will have clear action points to follow. These action points concern the requirements of responsible data projects. Civil rights organizations were justifiably concerned that[745] simply having abstract core values such as health, and even privacy, does not lead to responsible data projects in and of themselves. These organizations responded by defining the conditional requirements[746] that would

[742] Helberger, Natali and Sarah Eskens: Corona-app vraagt om meer toezicht op grote techbedrijven, in Volkskrant, 10.9.2020, online: <https://www.volkskrant.nl/columns-opinie/opinie-Corona-app-vraagt-om-meer-toezicht-op-grote-techbedrijven~b6898138/>
[743] See footnote 2
[744] https://www.nrc.nl/nieuws/2020/04/17/greoiende-kritiek-op-gehaaste-selectieprocedure-corona-app-a3997130
[745] https://www.veiligtegencorona.nl/burgerrechtenorganisaties-slaan-alarm-over-werkwijze.html
[746] They use the term "*uitgangspunten*". We translate it as "requirements" here, while the literal translation would be assumptions.

be needed for them to approve the development of a Corona app. If the DEDA requirements would have been met, the project team would have discovered many of these conditional requirements themselves. That being said, if the project team would have taken the necessary steps for an ethical assessment with the DEDA, it is likely that many of the conditional requirements would have already been met.

6.9 Explaining values

The third and final step of the DEDA is connecting the values of the relevant stakeholders to practical developmental decisions. As shown in the previous paragraphs, the absence of varied stakeholders and a clearly defined goal for the Corona app made it difficult to discover which values would be affected. If we stay within our thought experiment of a "Corona app project team" that would go through the DEDA, it would have discovered which values would be affected by their data project. If members had included the various signatories of the conditional requirements,[747] it would have become clear which values would need to be made explicit. Here are three examples of values mentioned in the conditional requirements:

One of the values explicitly and implicitly described is the efficacy of the app. This value would be made explicit in the beginning of the DEDA, with questions concerning the project goals and benefits. Another value that is important to the signatories is transparency. Transparency is an ambiguous value which can mean different things to different stakeholders. In the DEDA, transparency is made tangible through multiple questions. These questions concern how well the algorithms in use can be explained, and how to communicate the data project to the public. The last example of value could be equality. The signatories stress the need for the Corona app to be accessible to all, regardless of the mastery of the Dutch language or access to a smartphone. This value is made concrete in the DEDA by the questions concerning communications, but also in other questions concerning exclusion or discrimination.

This expert opinion does not try to distil all the values affected by a Corona app. The above examples show that by asking practical questions values are made explicit, becoming the foundation for a data project. In making these values explicit, stakeholders are able to check if the end result results of the app respect and represent these values. Of course, just because a stakeholder makes a value explicit does not mean it needs to be embedded in the design. Doing so would risk a natural fallacy with regards to value-sensitive-design (Manders-Huits, Zimmer, 2009). What the DEDA facilitates is a dialogue about these values, reflection by stakeholders, and attributing importance to the relevant values.

6.10 Conclusions

The development process of the *CoronaMelder* app was flawed, to say the least. In the case of the app and how the development process was set up, it ignored the political, value-laden aspects of data projects that require thorough public debate and reflection on the embedded values. As the analysis by Bits of Freedom, Waag, Platform Burgerrechten and Amnesty International shows, the most glaring requirement that the app failed to meet was neglecting to embed democratic values and human rights.[748]

What this expert opinion shows is that if the development of technological solutions to a (global) crisis is to be done responsibly, there has to be a dialogue discussing the values this solution represents. The Data Ethics Decision Aid is a tool that can aid in this process. Using DEDA does not impact the techno-solutionist rhetoric of politicians and policy makers, but it *can* be used to expose its shortcomings. By making design choices visible and linking them directly to values, DEDA demands discussion on the objectives and scope

[747] https://www.veiligtegencorona.nl/
[748] Veilig tegen Corona: https://www.veiligtegencorona.nl/toetsing-veiligtegencorona-criteria.pdf

of a project. It facilitates a process of thorough consideration through which possible harms, organisational challenges, design options, and most importantly, the broader range of societal impact can be addressed and documented appropriately.

This report and the thought-experiment of jumping back in time to the beginning of the development phase cannot change the outcome. Hopefully, it can steer the right people in the direction of a more thorough and comprehensive development process in case another techno-solutionist data project is introduced seeking to solve the next pandemic.

6.11 References

Coghlan, S., Cheong, M., & Coghlan, B. (2020). Tracking, tracing, trust: contemplating mitigating the impact of COVID-19 through technological interventions. *interventions*, *213*, 6-8.

Floridi, L. (2010). Information ethics. *The Cambridge handbook of information and computer ethics*, 77-99.

Floridi, L., Cath, C., & Taddeo, M. (2019). Digital Ethics: Its Nature and Scope. In *The 2018 Yearbook of the Digital Ethics Lab* (pp. 9-17). Springer: Cham.

Franzke, A.S., Muis, I. & Schäfer, M.T. (2021). Data Ethics Decision Aid (DEDA): a dialogical framework for ethical inquiry of AI and data projects in the Netherlands. *Ethics Inf Technol* https://doi.org/10.1007/s10676-020-09577-5

Manders-Huits, N., & Zimmer, M. (2009). Values and pragmatic action: The challenges of introducing ethical intelligence in technical design communities. International Review of Information Ethics, 10(2), 37–45.

Morozov, E. (2013). *To save everything, click here: The folly of technological solutionism*. Public Affairs.

Siffels, Lotje, David van den Berg, Mirko Tobias Schäfer, Iris Muis. 2021. Public Values and Technological Change: Mapping how municipalities grapple with data ethics. In Hepp, Andreas, Juliane Jarke, Leif Kramp (eds). *The Ambivalences of Data Power: New Perspectives in Critical Data Studies*. Palgrave. in print

Sweeney, Y. (2020). Tracking the debate on COVID-19 surveillance tools. *Nature Machine Intelligence*, *2*(6), 301-304.

Van Wynsberghe, A., Robbins, S. Ethicist as Designer: A Pragmatic Approach to Ethics in the Lab. *Sci Eng Ethics* 20, 947–961 (2014). https://doi.org/10.1007/s11948-013-9498-4

Zwitter, A. (2014). Big Data ethics. *Big Data & Society.* https://doi.org/10.1177/2053951714559253

7 Expert opinion: The Googlization of Pandemic Response: ethical concerns regarding digital contact tracing and big tech

Prof. Tamar Sharon, Interdisciplinary Hub for Security, Privacy and Data Governance, and Faculty of Philosophy, Theology and Religious Studies, Radboud University Nijmegen

7.1 Introduction

In April 2020, at the height of the COVID-19 outbreak and discussions on how to leverage digital technologies to contain it, Google and Apple released an API on which digital contact tracing apps could run. The “Google Apple Exposure Notification” (GAEN) framework came as a surprise. Not just because it was a first-time collaboration between the two tech giants, but because it adopted all of the technical specifications identified by privacy experts as necessary for privacy-preserving contact tracing. These included the use of Bluetooth for collecting and sharing non-traceable identifiers, and a decentralized data storage system. In the midst of heated national and international debates about the importance of privacy in relation to the roll-out of digital contact tracing, the GAEN framework was seen as victory on the side of privacy. This led to its widespread endorsement by leading privacy experts, including the DP-3T group (Tronscoso et al., 2020), the European Data Protection Supervisor, and numerous governments around the globe.[749] Currently, most national apps, as well as the Dutch *CoronaMelder*, run on this API.

While the GAEN framework offers important benefits in the attempt to automate contact tracing in privacy-preserving ways, the involvement of Google and Apple in this development raises concerns that governments have not properly addressed. These can be clustered under:

- *sectoral risks* – challenges to traditional public health expertise and a reshaping of pandemic response and public health practice and policy.
- *cross-sectoral risks* – novel dependencies on tech corporations for the provision of public goods across sectors in the public domain.

In both cases, there is an important legitimacy deficit on the part of tech corporations compared to the influence they exert within and across sectors. Furthermore, in both cases, the narrow focus on privacy and the protections offered by data protection law are insufficient to fully grasp and address these risks.

7.2 The “Googlization of pandemic response”

To understand the broader risks posed by Google’s and Apple’s involvement in the development of digital contact-tracing, it is important first to contextualize this involvement within a larger phenomenon of Big Tech’s push into (1) pandemic response, (2) the health and medical sector more broadly, and (3) into addi-

[749] Not all privacy experts agree that GAEN will deliver high levels of privacy. See for example, the analyses of Hoepman (2020), Jacobs, Boncz and Mekić (2020), and Boutet et al. (2020).

tional public sectors. In view of this, the GAEN framework is only one instance of a much larger trend in the increasing role tech corporations play in virtually all dimensions of social life.

1. The GAEN framework is only one of many ways that Big Tech—not just Apple and Google, but also Facebook, Amazon, Microsoft, Palantir and other subsidiaries of Alphabet, such as DeepMind and Verily—as well as their Asian counterparts including Alibaba, Baidu, Tencent and Huawei, have contributed to pandemic response strategies since the outbreak of COVID-19. Solicited by national governments (in the US, UK and China), or initiating involvement themselves, these pandemic response strategies have included, since March 2020: COVID-19 specific data collection, data analysis tools and AI diagnostics (Google, Facebook, Palantir, Alibaba, Baidu); the set-up of screening services and testing sites (Apple, Verily); donations of hardware: Chromebooks and WiFi hotspots to facilitate distance-learning (Google), tablets and patient monitoring devices (Amazon); the directing of funds amounting to hundreds of millions of euros for COVID-19 research (Chan Zuckerberg Initiative, Apple, Bill and Melinda Gates Foundation, Amazon); and most recently, the development of digital "vaccination passports" (Microsoft, Oracle), and involvement in vaccination programs (Verily).[750] The GAEN framework, while the most well-known and most global in its reach, is thus only one of the many pandemic response tools initiated by Big Tech.
2. Furthermore, the involvement of Big Tech in pandemic response is in itself an instance of a broader "Googlization of health", whereby these companies have become increasingly involved in both biomedical research and healthcare provision in the last six to seven years, mainly in the US but also in Europe and other parts of the world.[751]
3. And beyond this, the Googlization of health is indicative of the ever-growing involvement of Big Tech in many other public or otherwise essential sectors, such as education, urban planning, transportation and news provision (van Dijck et al. 2018).

While this trend poses obvious privacy and data protection risks, which policy makers, privacy activists and regulators have been laboriously addressing in recent years—an effort which has seen its culmination in the EU's adoption of the GDPR—it also poses a number of societal risks which have not been captured by the focus on privacy and data protection. These risks can be analyzed at two levels: challenges *within* the public health sector, or "sectoral risks", and risks to society at large relating to the increased involvement of Big Tech *across* sectors, or "cross-sectoral risks". As explained below, the GAEN framework is an example of both these types of risks.

7.3 Sectoral risks

1. Automating away important elements of the practice of contact tracing

Contact tracing is a time-tested method that has been successfully used to fight infectious disease outbreaks including syphilis, measles, HIV and Ebola, but which presents several limitations in its manual form. Namely, it is a labour-intensive practice in a situation of scarcity of human contact tracers. Particularly in the case of a virus like COVID-19, where infection can be asymptomatic for up to two weeks, its reliance on human memory makes it imperfect. Digital contact tracing seeks to address these limitations, and aims to make contact tracing faster, more efficient, and even more objective (insofar as it no longer relies on human memory) (CDC 2020; Ferreti et al. 2020). But the process of automation tends to reduce complex routine and professional tasks, such as contact tracing, to their most obvious functions. In this process norms and skills that are more implicit yet integral to a practice risk getting lost.

[750] For a more detailed overview of Big Tech's involvement in pandemic response see Sharon (2020).
[751] See Sharon (2016) and (2018) for more elaborate discussions on the "Googlisation of health".

As a practice, contact tracing involves a number of human skills which are not easily automated. First of all, the capacity to navigate complex human interaction. Contact tracers are trained to undertake epidemiological detective work to establish which contacts matter for disease contagion, based on things such as the environment that was shared with a person, the kind of activity that was being carried out at the time, and for how long. The replacement of this type of inquiry with the exchange of Bluetooth signals is problematic: Bluetooth cannot account for walls, it cannot control for environmental variables such as wind and ventilation, and some phones detect signals from up to 30 meters, without differentiating between 1 and 30 meters (Ada Lovelace Institute 2020). A case in point: the 15-minute criteria built into contact tracing apps means that a person may kiss or hug an infected individual for less than 15 minutes without the app picking this up. In other words, what constitutes a "contact" for a smartphone may not have epidemiological value, and vice versa. Human contact tracers can navigate the sea of potential false positives and false negatives in ways that apps simply cannot.

Second, the success of traditional contact tracing also rests on the ability of human contact tracers to build a relationship of trust with the interviewee. This is crucial for several reasons. Contact tracing is as much about identifying persons at risk of infection as it is about providing them with targeted information and walking them through the implications of this. Contact tracers need to deliver public health advice in a way that people will listen and act upon it, inquiring into the material conditions of the interviewee needing to sustain quarantine. Human skills are needed here, including empathy, patience and understanding, which are enacted in the back-and-forth of conversation between people, something an app can hardly do (Bourdeaux, Gray and Grosz 2020; Otterman 2020; Ross 2020). Thus, contact tracing has much more than a simple informative function, which is not easily automated.

For these reasons, it is crucial to include domain experts – in this case, epidemiologists and virologists, as well as public health officials, including human contact tracers – into the design process of a contact tracing app. In the case of the development of the *CoronaMelder* app, this was lacking. Indeed, among the participants of the appathon that the Ministry of Health, Welfare and Sport held in April 2020 to test competing apps, human contact tracers, those who understand the practice best, were missing. Moreover, in the early days of the development process, the Regional Public Health Services (GGD) raised concerns about the need for the app, at a time when they were busy scaling up manual contact tracing, as well as about the haste with which the Ministry had introduced it (Schellevis and van de Klundert 2020).

2. Technical expertise focused on privacy takes precedence over public health expertise focused on efficiency

The development of digital contact tracing was furthermore the arena for another clash of expertise, in which the involvement of Google and Apple became a determining factor: that between privacy experts and a number of public health, epidemiology and modelling experts. Public debate surrounding the development of a contact tracing app in many countries, including the Netherlands, was dominated early on by data protection and privacy concerns (Ienca and Vayena 2020; Joint Statement on Contact Tracing 2020; Ross 2020). And in the discussion on how to best design privacy into the apps' technical structure, decentralization became the standard-bearer for enhanced privacy (Troncoso et al. 2020). Decentralized storage, in which proximity contact information remains on users' phones, as opposed to centralized data storage, in which these data are stored on a central server (such as a national health authority's), was seen as key to the development of privacy-preserving contact tracing, and as inherently safer than centralization. In other words, as decentralization came to be equated with privacy-friendliness, centralization came to be equated with privacy-*unfriendliness*. However, as a number of public health experts have maintained, there are good reasons to opt for centralized data storage, though these have nothing to do with protecting privacy.

The most important of these arguments in favour of centralization goes back to the paucity of the epidemiological data collected by Bluetooth-based contact tracing in comparison to the context-rich data collected by human contact tracers. With a high risk of false positives and false negatives, a centralized approach, according to some public health officials, allows for better supervision and control of these data so that warnings are only sent out to people who have been in epidemiologically significant contact with an infected person (Kelion 2020, Leprince-Ringuet 2020). Too many false alarms can quickly result in people not paying attention to warnings sent by an app. Second, a centralized system also provides more overview of clusters of infections, by allowing to see where a cluster does or does not follow from an initial report of infection. Some experts have thus argued that a centralized system increases the likelihood of effective contact tracing. Considering that the effectiveness of digital contact tracing remains unclear, this is not trivial. In light of this, some scholars also argue that an evaluation of the benefits and disadvantages of centralized and decentralized systems should be made in relation not just to privacy harms but also in relation to the other harms which are at stake in the pandemic (e.g., loss of lives, economic damage, etc.) (White and van Basshuysen 2021).

Taking into account the advantages of centralized systems for public health, some scholars have argued for the need to focus on making centralized systems more secure, rather than opting for decentralized systems. For example, there is no reason per se why privacy and data security cannot be preserved in a centralized approach (Ilves 2020). Just as data collected by health authorities via manual tracing does not need to reveal the identity of infected persons, explore the nature of that contact, nor be shared with third parties, neither should this be the case in digital contact tracing.[752] Early on in the development of digital contact tracing there were indeed a number of countries developing apps based on a centralized system, including Germany, the UK, France, and Australia. For all of these countries except France, these systems were abandoned. Not necessarily because they could not identify contacts with sufficient accuracy, but to some extent because it became very difficult to design a functional app on Android phones and iPhones without the support of Apple and Google, which had already opted for the decentralized approach. In other words, Apple's and Google's choice for decentralization – a decision based on the arguments of privacy experts, rather than those of public health experts – determined how digital contact tracing would be carried out in a number of countries.

7.4 Cross-sectoral risks

1. Tech corporations become decision makers in national public health policy

In this way, Google and Apple not only had a decisive say in how a crucial public health measure would be rolled out, they also took a decisive position in a more political arena, by determining, sometimes against sovereign states, how public health policy should be shaped. In France, for example, which had been working on a centralized protocol, officials reported that when they found out about the Apple/Google API and tried to approach the companies to find workarounds, their attempts were met with staunch reaffirmations that the companies would only work with decentralized technologies (Scott et al. 2020). For a country like France, which insisted on pursuing its national centralized system, this meant open confrontation with the tech companies, and being portrayed in the media as caring less about privacy than the tech companies did (Hern 2020). One French official has been quoted as saying that "European states are being completely held hostage by Google and Apple," (Rosemain and Busvine 2020). Similarly, a representative of the Latvian government has openly described discussions with the companies as running "into a Silicon Valley-built brick wall" and has questioned the extent to which Google or Apple should "get to tell a democratically elected government or its public health institutions what they may or may not have on an app" (Ilves 2020). Such frustrations around the need to comply with the rules set out by the companies have been echoed in other countries and federal authorities as well, including the UK and North Dakota in the US (Tokmetzis and Meaker 2020). Effectively, Apple and Google did not just

[752] Of course, the data breach in the Dutch GGD IT system revealed in January 2021 does not help the case for centralized data storage, but this is exactly a reason to improve the data security of such systems.

contribute their technical expertise to the pandemic response, but also determined which path an important global public health policy would take, setting down the conditions for which apps could exist and how governments should use them.

2. The instrumentalization of privacy

In this context, it is important to critically question why Google and Apple chose first to develop an API rather than an app, something they could have easily achieved. And second, why privacy protection, symbolized by their choice for supporting only apps that use decentralized rather than centralized data storage systems was so pivotal. Thomas Kuipers (2020), a Science and Technology Studies scholar, has argued that Google's and Apple's decision to develop an API and not an app was a skillful way for the companies to present their involvement as merely technical, not political. It allowed them to demonstrate their willingness to contribute to a major societal problem – the pandemic – and their capacity to do this quickly and efficiently, while avoiding getting involved in complicated political discussions and controversies about the development of the apps themselves.[753] Indeed, if Google and Apple were also competing alongside local startups in the Dutch appathon, the appathon would have looked completely different. And if their prototype had won the competition, which would be expected, this would have looked very bad for the government, favouring large American corporations over local ones. In other words, by developing an API and not an app, Google and Apple succeeded in determining an important dimension of pandemic response in the Netherlands and other countries, without ever engaging in pandemic response controversies and decision-making, further contributing to a veneer of neutrality.

As to the second question, for tech companies, privacy-friendliness has increasingly become a means of gaining credibility in a highly competitive market. Apple in particular has boldly branded itself as a champion of privacy and data-security, mostly in contrast to Facebook and the ad-tech industry in general, but also in terms of its support of the GDPR and the need for similar regulation in the US (Lomas 2021). While Google may lag behind in these attempts, and its ad revenue-related business model has been highly criticized for privacy infringing data practices, it is important to understand that this is no longer the sole or even main modus operandi required for Google or other tech corporations to achieve their ambitions. Indeed, while these companies' business models, certainly when it comes to health-related initiatives, are not always transparent nor well-developed yet, it is clear that a number of their activities do not require using data in ways that are privacy unfriendly, and some of them do not require the use of data at all.

A good example of such products and initiatives that tech corporations are developing for the health and medical sector which do not require any repurposing of data is Apple's ResearchKit. Launched in 2014, ResearchKit software allows medical researchers to carry out clinical studies using the iPhone as a means for collecting data. Apple does not need to see, control, analyse or in any way handle the data being collected in the context of these studies in order for the ResearchKit software and the iPhone, as a new tool for remote clinical studies, to be a success. Another example is the predictive algorithms and digital biomarkers that some of these companies, including a number of Alphabet subsidiaries, are developing for health and medicine. While large amounts of health data are required to train these algorithms, companies do not need to peddle in data sharing with third parties in order to monetize these efforts. Monetization will come at the point of selling the algorithms developed using these data or selling access to these algorithms to the medical and public health sector. In other words, privacy, which has for long been the main contentious issue at stake for citizens in relation to Big Tech's business models, is a non-issue in some of their more recent business models, certainly when it comes to public health. In this context, privacy-friendliness may act as a smokescreen, allowing these companies to make bigger and broader inroads into public sectors like health and the pandemic response. Ultimately, then, the privacy

[753] This positioning of tech companies as "neutral intermediaries" is reminiscent of how social media platforms such as Facebook and Twitter portray themselves as mere facilitators in public and political debate rather than active agents in its formation, and the associated risks this can have for democracy (see e.g., Helberger 2020).

friendly GAEN framework can be seen as a "wolf in sheep's clothing" facilitating greater entrenchment in the realm of global public health.

3. Increased dependency on non-accountable private actors

Most importantly, the narrow focus on privacy enables these companies to increase their infrastructural power across sectors, moving from the tech sector to public health, education, transportation, urban planning, immigration control and others. Indeed, tech corporations are no longer just the producers of isolated IC technologies, hardware and software, but of *computational infrastructures*, that involve a network of integrated software platforms, data centers, cloud infrastructure and devices (van Dijck et al. 2018; Gürses and Dobbe 2020). If traditional infrastructures have been thought of as physical structures that organize social life, such as electrical grids, highways or sewage systems, increasingly, a layer of computational infrastructure has become no less essential to the organisation and coordination of contemporary social life. At least in Europe, traditional infrastructures tend to be run by the state or outsourced to private companies regulated by the state. In contrast, computational infrastructures are owned by a handful of tech corporations which are not accountable in the way that states are (Sharon 2020).

As Taylor (2021) argues in her work on the legitimacy deficit of private actors from the technology sector taking over public sector functions traditionally carried out by governments, this situation is complicated by the fact that private actors tend to function outside the normative and legal frameworks that make states accountable to their citizenry in democratic nations, including mechanisms such as public scrutiny and recurring democratic elections. This allows tech corporations to claim a passive kind of political legitimacy, all the while being shielded from the demands of accountability that come with their involvement in the public sector. Furthermore, a recent history of under-investment and cuts in public sector capacities in liberal democracies, including historical welfare states like the Netherlands, has contributed to weakened public institutions and increased opportunities for tech corporations to move into the public sector (Mazzucato 2018). An example of this is the difficulty of carrying out mass test and tracing during the pandemic.[754]

The growth of computational infrastructural power that Big Tech has been enjoying in recent years, and which allows them to increase their power not only within but also across sectors, is accompanied by important risks. First, it creates new dependencies on Big Tech for the delivery of public goods across sectors of social life. Infrastructures are hard to remove or bypass (think of a country's system of roads) and they create new path dependencies which make them unavoidable. The GAEN framework is a case in point, which actually shows to what great extent this dependency is already a reality: it is all but futile today to try to build an app that would not run on either the iOS (Apple) or Android (Google) smartphone operating systems, or to build an app that would not make use of existing cloud services. Such an app would not be interoperable with those from other countries – an obvious benefit for contact tracing – and it would be difficult for it to reach a large number of people, another necessity for efficient contact tracing. The computational infrastructures that have been developed by and for the tech sector in this way become unsurpassable in new sectors, such as public health. Second, the burgeoning involvement of Big Tech in ever new public sectors will likely be accompanied by a lack of transparency. Firms function in the realm of business contracts and business ethics, which are more easily shielded from public scrutiny than public sector contracting. This situation limits possibilities for contesting and redress when something goes wrong. Third, like all technologies, computational infrastructures come with their own set of values and aims, and certainly in the case of Big Tech, with an expansive political economy to boot (Gürses and Dobbe 2020). While the involvement of these companies in the shaping and delivery of public goods

[754] The UK actively sought the help of Palantir in this respect, while in the US, New York Governor Andrew Cuomo announced partnerships with former Google CEO Eric Schmidt and the Bill and Melinda Gates Foundation to help leverage technology to shape NY's post-COVID reality, including education.

may serve the public interest, this is not a given. We can expect that enhancing their own profits will be a primary ambition for these companies getting involved in the public sector, possibly at the expense of the public good.

7.5 Conclusions and recommendations

The increasing involvement of Big Tech in sectors such as public health poses a number of risks at the sectoral and cross-sectoral levels. Sectoral, insofar as these companies increasingly replace traditional, sectoral experts in decision-making processes, thus contributing to a reshaping of the sector they are moving in to and where they lack the legitimate expertise to do so. Cross-sectoral, insofar as these companies increasingly contribute to political decision-making, for example in the realm of national and global public health policy, and insofar as their computational infrastructures have become essential for the functioning and coordination of increasing aspects of social life. Here, they lack legitimacy in terms of the accountability that comes with assuming state functions, such as the delivery of public goods. The GAEN framework, as has been shown here, is an instance of these developments and their accompanied risks. In the context of a pandemic, where society's dependency on digital infrastructures for mediated human contact grows – for work, schooling, health consultations, and socializing – these risks are even greater. In this light, the following recommendations are proposed:

Sectoral

- Always include domain experts in the design process for automating complex practices (e.g., in "participatory design"). In the case of digital contact tracing apps, not just public health experts and epidemiologists, but also include manual contact tracers themselves. This can prevent crucial sectoral values, skills and norms from being "automated away".
- Ethical considerations concerning public health interventions should be broad. Privacy is an important concern but should be weighed against other ethical principles, as well as the necessity and efficiency of the intervention.

Cross-sectoral

- While privacy and data protection concerns are not to be minimized in the context of digital tools and private actors, privacy law and data protection regulation are insufficient to address the breadth of the societal risks identified here. Furthermore, the focus on privacy may act as a smokescreen that enables these pernicious developments. As the digitalization of society advances, and as Big Tech increasingly moves into new sectors, this understanding must become integral to our engagement with digital technologies and tech corporations.
- In light of this, regulation that focusses on securing the public good (not just individuals' personal data) should be further developed in relation to digitalization, with an eye on protecting public values, including democratic legitimacy, universal access, justice and fairness.
- Apply and demand a thick account of legitimacy and public accountability to tech corporations acting in the public realm. Amongst others, by ensuring that in any situation in which tech companies take over traditional public functions, the public interest remains (at least one of) the primary aims, that governments maintain regulatory oversight, that contracts and implementation are open to public scrutiny, and that possibilities for opting out and redress exist.

7.6 References

Ada Lovelace Institute (2020). *Exit Through the App Store*. https://www.adalovelaceinstitute .org/our-work/COVID-19/COVID-19-exit-through-the-app-store/.

Bourdeaux, M., M. Gray, B. Grosz (2020). The best tech for contact tracing? Systems designed for healthcare workers. *Interactions.* https://dl.acm.org/doi/pdf /10.1145/3406775?casa_token=VMQZ5nS0fzAAAAAA:alyxE4hWdfF _RW8tekyT2slHAVKdz8rLjZ02UzFATYmdkdU-1JTQ9I8Ubrdrk3liwvxuOt3iBUcjp6s

Boutet, A., C. Castelluccia, M. Cunche, A. Dmitrienko, M. Miettinen, T. Duc Nguyen, V. Roca, et al. (2020). Contact tracing by giant data collectors: opening Pandora's Box of threats to privacy, sovereignty and national security. https://hal.archives-ouvertes.fr/hal-03116024v1

Centers for Disease Control and Prevention (CDC) (2020). *Digital Contact Tracing Tools for COVID-19*. https://www.cdc.gov/Corona virus/2019-ncov/downloads/digital-contact-tracing.pdf.

Ferreti, L. et al. (2020). Quantifying SARS-CoV-2 transmission suggests epidemic control with digital contact tracing. *Science,* 368, 6491.

Gürses, S. and R. Dobbe (2020). Programmable infrastructures. TU Delft. https://www.tudelft.nl/en/tpm/ programmable-infrastructures/

Helberger, N. (2020). The political power of platforms: How current attempts to regulate misinformation amplify opinion power. *Digital Journalism* 8(3): 1-13. DOI: 10.1080/21670811.2020.1773888

Hern, A. (2020). France urges Apple and Google to ease privacy rules on contact tracing. *The Guardian*, April 21. https://www.theguardian.com/world/2020/apr/21 /france-apple-google-privacy-contact-tracing-Corona virus

Hoepman, J.H. (2020). Stop the Apple and Google contact tracing platform (or be ready to ditch your smartphone). https://blog.xot.nl/2020/04/11/stop-the-apple-and-google -contact-tracing-platform-or-be-ready-to-ditch-your-smartphone/.

Ienca, M., and Vayena, E. (2020). On the responsible use of digital data to tackle the COVID-19 pandemic. *Nature Medicine* 26, 463–464. https://doi.org/10.1038/s41591-020-0832-5

Ilves, I. (2020). Why are Google and Apple dictating how European democracies fight Corona virus? *The Guardian*, June 16. https://www.theguardian.com/commentisfree/2020/jun/16 /google-apple-dictating-european-democracies-Corona virus?CMP=Share_AndroidApp_Tweet.

Jacobs, B., P. Boncz and D. Mekić (2020). Een App als Digitaal Hulpmiddel: Achtergrond bij Traceren en Informeren. http://docplayer.nl/189816449-Een-app-als-digitaal-hulpmiddel -achtergronden-bij-traceren-en-informeren-1-concept.html

Joint Statement on Contact Tracing (2020). https://www.esat.kuleuven.be/cosic/sites /contact-tracing-joint-statement/

Kelion, L. (2020). NHS rejects Apple-Google Corona virus app plan. *BBC*, April 27. https://www.bbc.com/news/technology-52441428.

Kuipers, T. (2020). The Politics of Contact Tracing Apps: How Apple and Google distance themselves from politics while building a global infrastructure of contact tracing. https://blog.sts.univie.ac.at/2020/07/15/the-politics-of-contact-tracing-apps/

Leprince-Ringuet, D. (2020). The world's first contact-tracing app using Google and Apple's API goes live. *ZDNet*, May 28. https://www.zdnet.com/article/the-worlds-first-contact-tracing-app-using-google-and-apples-api-goes-live/

Lomas, N. (2021). Apple's Tim Cook warns of adtech fueling a 'social catastrophe' as he defends app tracker opt-in. *TechCrunch*, January 28. https://techcrunch.com/2021/01/28/apples-tim-cook-warns-of-adtech-fuelling-a-social-catastrophe-as-he-defends-app-tracker-opt-in/

Mazzucato, M. (2018). *The Value of Everything: Making and Taking in the Global Economy.* Penguin Books.

Otterman, S. (2020). As the Nation Begins Virus Tracing, it Could Learn from this N.J. City. *The New York Times*, May 21. https://www.nytimes.com/2020/05/21/nyregion/contact-tracing-paterson-nj.html.

Rosemain, M. and D. Busvine (2020). France, Germany in standoff with Silicon Valley on contact tracing. *Reuters*, April 24. https://www.reuters.com/article/idUSKCN2262LM

Ross, C. (2020). 5 burning questions about tech efforts to track COVID-19 cases. *STAT,* April 18. https://www.statnews.com/2020/04/15/Corona virus-digital-contact-tracing-tech-questions/.

Schellevis, J. and M. van de Klundert (2020). GGD twijfelde lang over nut CoronaMelder-app en waarschuwde voor haast. *NOS Nieuws*, October 19. https://nos.nl/artikel/2352923-ggd-twijfelde-lang-over-nut-Coronamelder-app-en-waarschuwde-voor-haast.html

Scott, M, Braun, E. Delcker, J. and Manancourt, V. (2020). How Google and Apple outflanked governments in the race to build Corona virus apps. *Politico*, May 15. https://www.politico.eu/article/google-apple-Corona virus-app-privacy-uk-france-germany/

Sharon, T. (2016). The Googlization of health research: from disruptive innovation to disruptive ethics. *Personalized Medicine* 13(6), 563-574.

Sharon, T. (2018). When digital health meets digital capitalism, how many common goods are at stake? *Big Data & Society.* https://doi.org/10.1177/2053951718819032

Sharon, T. (2020). Blind-sided by privacy? Digital contact-tracing, the Apple/Google API and big tech's newfound role as global health policy makers. *Ethics and Information Technology.* https://doi.org/10.1007/s10676-020-09547-x

Troncoso, C. M. Payer, J-P. Hubau, M. Salathé, J. Larus, E. Bugnion et al. (2020) Decentralized Privacy-Preserving Proximity Tracing. Available from: https://arxiv.org/abs/2005.12273

Taylor, L. (2021). Public actors without public values: Legitimacy, domination and the regulation of the technology sector. *Philosophy and Technology*. https://doi.org/10.1007/s13347-020-00441-4

Tometzkis, D. and Meaker, M. (2020). We were told technology would end COVID-19 lockdowns, but the truth is there's no app for that. *The Correspondent*. https://thecorrespondent.com/502/we-were-told-technology-would-end-COVID-19-lockdowns-but-the-truth-is-theres-no-app-for-that/66389901600-2c9929bb

Van Dijck, J., T. Poell and M. de Waal (2018). *The Platform Society: Public Values in a Connected World.* Oxford: Oxford University Press.

White, L., and P. van Basshuysen (2021) Without a trace: Why did Corona apps fail? *Journal of Medical Ethics*. https://doi.org/10.1136/medethics-2020-107061.

8 Expert opinion: CoronaMelder: an economic perspective

Expert opinion by Joost Poort, Associate Professor, Institute for information Law (IViR), University of Amsterdam

8.1 Introduction

The COVID-19 pandemic triggered a host of interventions across the globe that had a profound impact on daily life, civil liberties and the economy. In the Netherlands, schools were closed as well as restaurants, cinemas, theatres, libraries, sporting facilities and most shops. Public, sports and cultural events were cancelled or postponed. International travel was discouraged, and some borders were even closed, while people who nevertheless did travel abroad were urged to go into quarantine. A curfew was imposed, restrictions were introduced on the number of visitors one could receive at home, as well as the number of people that were allowed to gather in public spaces and the number of attendees at weddings and funerals. Wearing a protective mask was made compulsory in public transport, shops and most other public or semi-public buildings, while social distancing – keeping anyone from outside your household at a minimum distance of 1.5 meters – became the norm.

What all these intrusive measures have in common is their aim to prevent the spread of the virus and its devastating effects on public health and the health care system by *generically* reducing the number of contacts that can cause the virus to jump from one host to the other.

In addition to such measures, contact tracing has been used to identify those that have been close to someone who tested positive for the virus and thus run a *specific* risk of being infected. The aim of contact tracing is to identify infected people at an early stage, prevent them from having further contacts and thus, infect others before developing symptoms. Potentially, this leads to a more precisely targeted reduction in contacts, namely contacts with a higher likelihood of leading to new infections, than generic measures that reduce the number of contacts in society at large.

In economic terms, the effects of the generic measures mentioned above were immediate and immense. In December 2019 and pre-pandemic, CPB predicted the Dutch economy would grow by 1.3% in real terms in 2020, with the largest perceived threats to growth being issues concerning nitrogen- and PFAS-norms, Brexit and finally, US trade policy (Centraal Planbureau 2019). Half a year later, in June 2020, it predicted an unprecedented decline of 6% in real terms (Centraal Planbureau 2020). The most recent forecast from March 2021 was slightly more optimistic, estimating the decline in 2020 at 3.7% and predicting a recovery of 2.2% in 2021 (Centraal Planbureau 2021). Meanwhile, public expenses have skyrocketed. Billions were spent on medical care and on support for those sectors of the economy that were forced to shut down, causing government debt to grow rapidly.

And these are just the monetary and short-term effects. The effect of cancelled and postponed medical care during the first COVID-wave in 2020 in the 12 most frequently provided medical specialties was estimated at 34-50,000 healthy life years lost (van Giessen et al. 2020, p. 3). This number excludes many effects, such as the negative effect on the early diagnosis of cancer due to halting public screening programmes. Also, economists have warned about long-term economic effects, for instance those of the temporary closing of schools (Teulings 2021) and have warned that the current interventions aimed at stopping or slowing down the spread of the virus are overstated, causing more costs than benefits to society (e.g., Baarsma et al. 2021). On the other hand, early attempts at the cost-benefit analysis of restrictive measures in the United States have turned out to be positive. Doti (2021) estimates the reduction in the number of lives lost in the US at 358,000 in 2020. At an age-adjusted value of statistical life (VSL) of $4.2 million, this outweighs the estimated costs of lost jobs and negative income effects by a factor 3.7.[755] Broughel and Kotrous (2021) reach similarly positive net outcomes of the restrictive measures during the pandemic's first wave.

Against this background, this paper analyses digital contact tracing apps, specifically the Dutch *CoronaMelder* through an economic lens. Like many countries before it, the Netherlands launched an app for digital contact tracing in October 2020. The aims of this smartphone app are: (1) to assist or supplement public health institutions (GGD) in tracing the recent contacts of someone who tested positive for COVID-19, which may have led to new infections; (2) to slow down the spread of the virus by urging these contacts to be tested and quarantine until it is clear whether or not they have been infected, in order to stop them from infecting others (Ebbers et al. 2021, p.3).

The structure of this expert opinion is as follows: Section 2 describes several basis characteristics of the *CoronaMelder* app and its usage and summarizes the conclusions of the recently published evaluation. Section 3 discusses the private costs and benefits of using the app: what are the incentives for an individual to use it? Subsequently, Section 4 looks at the direct and indirect costs and benefits from a societal perspective. Section 5 concludes the report.

8.2 Facts and figures about the *CoronaMelder* and conclusions from evaluation

One of the first foundations for the use of contract tracing apps to combat COVID-19 was provided by Ferretti et al. (2020). Based on models of the spread of the epidemic and observing that a large proportion (46%) of new infections resulted from pre-symptomatic individuals, the authors concluded that manual contact tracing would not lead to epidemic control. They proposed the introduction of an app to immediately notify the previous contacts of a person who turned out to be positive. This could reduce the need for more restrictive measures. This idea gained traction rapidly. China, South Korea, Israel and Singapore were among the first countries to introduce such apps, followed in Europe by Germany and Switzerland and several countries afterwards (Rehse and Tremöhlen 2020, p. 36-37).

In the Netherlands, the CoronaMelder app was officially launched on 10 October 2020. Installing the app is voluntary (there is no obligation or pre-installation on new phones), and after being tested positive,

[755] Note that this analysis disregards various costs and benefits, such as the aforementioned costs of postponed medical care and long-term educational effects, as well as the benefits of preventing long-term health damage for long-COVID patients, and of a further surge in medical costs treating patients.

users can consent to alerting their past contacts via the app.[756] The app registers a contact when another app user is estimated to have been within 1.5 m for at least 15 minutes.

On 28 May 2021, an evaluation of the *CoronaMelder* was published (Ebbers et al. 2021), which is taken as the basis for most of the factual information in this section. Some key figures as per 23 May 2021:

- 4.9 million people downloaded the *CoronaMelder*, which corresponds to 28% of the population.
  - This number increased rapidly shortly after the launch in October and has leveled off since. No net decline had been reported so far.
  - The percentage of app users is roughly stable across age groups but increases with education level.
  - An estimated 2.9 million people (around 17% of the population) actually *use* the app.
- 174,000 infected people notified their contacts via the *CoronaMelder* (3.6% of the installed base).
- 189,000 people applied for a test after a notification in the app.
  - 77% of these had not or not yet been reached via manual contact tracing.
- 14,000 people tested positive after receiving a notification.

The evaluation by Ebbers at al. (2021) reaches the following conclusions:

- More than half of the people who applied for a test after a notification in the app were never notified by GGD. Without the app, this group would not have been identified, or only after they developed symptoms. Another group was notified by the app before they had been reached by traditional contact tracing enabling them to avoid further contacts and to apply for a test earlier.
- About 3-5% of people who applied for a test after a notification in the app but who did not have symptoms tested positive, as opposed to around 1% in the general population.
- Overall, around 1 out of 10 test applications and 1 out of 20 positive tests was triggered by the CoronaMelder. Between 26 September 2020 and 18 April 2021 this amounted to around 11,000 positive tests triggered by the app, while around 128,000 negative tests were triggered by the app.
- Modelling by RIVM indicates that the app prevented more than 15,000 infections and over 200 hospitalisations between December 2020 and March 2021 (based on 7,500 positive tests triggered by a notification).
- 97% of app users state they were willing to stay home upon such instruction by the app and 95% would take a test. In practice, these numbers were considerably lower: 45% of the people who received a notification actually stayed home, while 41% took a test.

Overall, the authors conclude that the app had a small but noticeable added value. They state that the fact that it is small is understandable, given the limitations to social life since the introduction of the app. This implies that as restrictions continue to be rolled back in the coming months, the added value of the *CoronaMelder* will be expected to increase. It might increase further if more people are convinced to use the app, if the time between contacts and notifications decreases, and if compliance with instructions upon notifications is improved.

Ebbers et al. (2021) also pay attention to the unintended effects of the app. App users might, for instance, feel overly safe, resulting in non-compliance with other measures. The authors find no indications for

[756] Around 75% of positively tested app users indeed shared their key. This is likely an underestimation of the willingness to do so, since contact tracing employees do not always ask about the use of the *Coronamelder* (Ebbers et al. 2021, p. 19).

this and consider it unlikely. They do, however, find indications that some people feel public pressure to install and use the app.[757] Lastly, they mention the issue of false positives, for instance, when signals travel through walls.

The authors (p. 26-27) point out that international studies show that contact tracing apps can be more effective than manual contact tracing and can help reduce the reproduction rate R^0, the number of infections and the death toll. These insights are based on modelling rather than empirical studies, however.

8.3 Incentives for using digital contact tracing apps

Compliance with most measures mentioned in the introduction benefit individual and public health simultaneously, provided they are indeed effective in preventing the spread of the virus. For instance, by respecting social distancing rules, an individual reduces both the risk of contracting the virus, and the risk of infecting others. Vaccination has a similarly symmetric effect, benefitting both the person receiving the vaccination, and his or her future contacts.[758]

Digital contact tracing apps are fundamentally different in that respect. The app does not prevent the user from being infected. Therefore, under the assumption that early and often pre-symptomatic knowledge of a possible infection has no effect on treatment and recovery, there are *no personal health benefits for a user of the app*.

What the app does do is increase the likelihood of early detection of being infected and by doing so, enables a person to take action to prevent spreading the virus further. Therefore, installing the app is something one does for the health of others (or in response to social pressure to that end). Potential health benefits fall on the contacts a person would have had and via them to others whom they might have infected, while potential costs fall on the person installing the app. This is very comparable to the classic public good problem, in which people are unwilling to invest in public goods (non-rival and non-excludable goods) and prefer to free-ride instead.

Of course, the potentially positive health effects for contacts as well as for society at large can still be a valid incentive for a person to install the app. In economic terms: a person can derive utility from contributing to the health of their relatives and others and of 'being a good citizen'[759] (see also the empirical findings in section 9). On top of this, there is an indirect effect: that by doing so, one contributes to the re-opening of society, which also brings private benefits to most people. Indeed, a consumer survey indicates that 47% of the *CoronaMelder* users agree with the statement that using the app makes one a good citizen, opposed to 14% of people who stopped using the app and 9% of non-users (Ebbers at al. 2021, p. 53). A similar pattern is found for the statement that using the app helps the economy. Agreement levels with the statement that the app helps protect people with vulnerable health is substantially higher at 78% among users of the app. Interestingly, 34% of non-users and 41% of previous users also agree with the latter statement. This raises the question whether these groups consciously decide *not* to contribute to that protection, or fail to understand that such protection is provided when *others*, not just vulnerable groups, install the app. There are strong network externalities associated with installing the app: if more

[757] This is in line with the monitoring framework (see chapter 9) which found that people do not feel pressure from the government or their employer to install the app, but many people – in particular younger age groups – often feel morally obliged to install the app.

[758] Note, however, that the size of these effects in both directions may differ, depending on the age and overall vulnerability of a person. Young, healthy people have relatively little to fear from being infected compared to elderly people, whereas their disutility from social distancing is likely to be larger. This implies that the net individual incentive for complying with generic measures as well as the incentive for taking a vaccination is considerably smaller for younger age groups in good health – hence clandestine 'Corona parties'.

[759] In the behavioural economic literature, this is referred to as the 'warm glow' of giving (coined by Andreoni, 1989).

people install the app, the chances increase that the contacts of an infected person will be detected.

Whereas these potential benefits of the app are primarily indirect, the potential costs fall on the user. So, what are the potential costs for the person installing the app? In monetary terms, the app is free. However, installing the app requires one to 'spend' a minute or so via a mobile connection, and spend a few MB of data credit, as well as storage space on the smartphone. Once installed, the app continues to use data to check periodically for possible infectious contacts and requires Bluetooth to remain active, which adds to battery depletion (despite the fact that the app uses 'Low Energy Bluetooth'), possibly contributing to the nuisance of having to rechange at an inconvenient moment, on top of the actual energy costs of recharging.

These are all very minor disincentives for installing and using the app, but in the absence of private benefits, they might still contribute to the relatively low level of adoption seen in the previous section. What is more, these 'costs' appear to be overestimated by non-users: 22% of them think it would cost a lot of time and energy to install the app (opposed to 3% of users) and 49% of non-users expect the app to be user friendly (opposed to 99% of users) (Ebbers at al. 2021, p. 16-17). Overall, users of the app often see personal advantages (67%) and rarely disadvantages (7%), while non-users rarely see personal advantages (9%) and more often disadvantages (24%).

Privacy concerns are a more profound category of private 'costs' associated with installing the app. Survey results show that such concerns correlate strongly with app usage, while there are widely spread misconceptions of the privacy aspects of the app itself. Amongst app users, 85% believe personal information is kept strictly confident, while only 55% of non-users think so. Nevertheless 57% of app users think the apps records the user's location; within the group of non-users, this is 68%. Remarkably, this misconception is more common among higher educated groups. Along the same lines, 35% of app users and 55% of non-users mistakenly think the app records their name and personal data.[760]

Reducing these misconceptions by providing better information will likely be helpful to improve the adoption rate of the app. However, to some extent, self-justification will play a role here: people who did not install the app for whatever reason soothe their consciences by stating it would be very complicated and time-consuming to do so. In such cases, providing better information would be of little help. Moreover, adoption rates comparable to that in the Netherlands have also been observed in other countries, such as Germany and Switzerland (Rehse and Tremöhlen 2020, p. 2, 38).

To conclude this section: the asymmetry between the costs and benefits of app usage remains a fundamental obstacle for large-scale voluntary adoption. It is the classic public good problem all over again. For that reason, it remains essential to reduce the actual and the perceived personal costs of using the app. Particularly in relation to privacy issues, misconceptions about how the app works could be reduced by providing better information, which will likely be helpful to improve the adoption rate of the app. From an economic perspective, even subsidizing app users to compensate them for the positive externalities of installing and using the app could be justified, although care should be taken not to damage intrinsic motivation in this way (see also: Rehse and Tremöhlen 2020, p. 24-27). One way to do this might be a lottery amongst active app users, like the State of Ohio did with people who were vaccinated, leading to a substantial increase in the vaccination rate.[761]

[760] See also monitoring framework. See chapter 9.

[761] See: https://odh.ohio.gov/wps/portal/gov/odh/media-center/odh-news-releases/odh-news-release-05-20-21.

8.4 Towards a social cost-benefit analysis

Now it is time to develop a more comprehensive economic perspective on the direct and indirect social costs and benefits of the *CoronaMelder* app. While a full social cost-benefit analysis (CBA) does not fall within the scope of this expert opinion, a few rudimentary steps have been taken in this section.

An important and non-trivial starting point for any such analysis is the counterfactual: what is the next best policy or course of action relative to which costs and benefits are assessed? As mentioned above, Ferretti et al. (2020) proposed digital contact tracing apps as an alternative to more restrictive measures. However, such a counterfactual statement would entail not only analysing the effects of the app in greater detail, but also those of the other measures at stake. It was also mentioned in the introduction that some people claim that for several of these generic measures, the costs outweigh the benefits. If that was the case, such counterfactuals would flatter the picture for contact tracing apps. Alternatively, the two CBAs mentioned in the introduction establish sound benefit-to-cost ratios for the generic package of restrictive measures in the US, which would imply an unnecessarily high benchmark for the app. Therefore, it is preferable either to look at the alternatives of 'more intensive manual contact tracing' or 'doing nothing'.

8.4.1 Costs and benefits relative to doing nothing

If 'doing nothing' is considered the next best course of action, one should start by taking stock of all the societal effects of the app. On the cost side of the balance sheet are the costs of developing and maintaining the app, and of the publicity campaign held to promote it. Based on information from the Health Ministry obtained by the project team in november 2020, these costs were €12.6 million (€5 million for development, €2.8 for communication, €3 for maintenance/operation, €1.8 for policy).[762]

Additional costs are the unintended effects as mentioned by Ebbers et al. (2021): the disutility of the public pressure some people feel and privacy concerns, as well as the energy and data consumption of installing and using the app. On top of that, false notifications lead to substantial time and costs wasted on testing and self-isolation.

Most of these effects are hard to quantify, let alone express in euros without extensive research. However, an effort can be made to tentatively estimate the social costs of the latter, assuming that all negative tests triggered solely by the app would not have taken place without it. As was mentioned in Section 2, this amounts to 128,000 tests between 26 September 2020 and 18 April 2021. So, what are the total social costs of a negative test?

First, there are the actual cost of the test itself including its analysis. Since no detailed information about the costs of official GGD-testing (and manual contract tracing) are available, rough estimates have to be made. Currently, commercial PCR tests are advertised in the Netherlands at prices from €75. Assuming a profit margin of 15% gives a cost estimate of €65 per PCR test. GGD testing may operate at lower costs, given the substantial economies of scale it benefits from.

Added to that are the time costs of taking the test and the inefficiencies/loss of utility from self-isolation until the negative result is available. For the purpose of this estimate, it is assumed here that on average a working day is lost in this way, valued at the average gross wages in the Netherlands, which was €24/hour in 2020.[763] Thus, the total welfare costs of a negative test prompted by the *CoronaMelder* will be in the

[762] In a full-blown CBA, these costs figures warrant further scrutiny. For instance, there may be additional costs of the app at the end of the municipal health services (GGD). On the other hand, some of these costs directly lead to benefits for other economic actors, most notably the costs of advertising which consist largely of scarcity rents.

[763] See: https://www.cbs.nl/nl-nl/visualisaties/dashboard-arbeidsmarkt/ontwikkeling-cao-lonen/uurloon. Again, this is a ballpark estimate. On the one hand, the average productivity of employees exceeds these gross wages, so if a full day's work is lost, the costs will be larger. On the other hand, the costs associated with those who are retired, going to school or not working for other reasons will be smaller.

order of 8×€24 + €65 = €257. The total costs of 128,000 such false alerts between 26 September 2020 and 18 April 2021 amounts to €33 million. The full costs of the app and testing due to false alerts combined add up to around €46 million. Including the costs of testing positive cases, these are around €48 million.

On the positive side are the welfare gains of preventing infections. Section 2 mentioned the estimate by RIVM that the app prevented more than 15,000 infections and over 200 hospitalisations between December 2020 and March 2021. Extrapolating this to September-April to compare the costs and benefits over the same time span would lead to the prevention of more than 22,000 infections and around 300 hospitalisations.[764]

An alternative way to arrive at an estimate for the number of prevented infections is via the 11,000 positive tests triggered by the app: Assume a reproduction rate R^0 which is constant over time at 0.9 (in fact, it has been larger than 1 for considerable periods between September 2020 and April 2021). And assume that an infected person notified by the app manages to halve this to 0.45, after which the chain of infection continues at the 'ordinary' reproduction rate of 0.9. Then each positive test triggered by the app prevents 0.45 × (1 + 0.9 + 0.92 + …) = 4.5 subsequent infections. At an R^0 of 0.8 this would add up to 2. Correspondingly, 11,000 positive tests triggered by the app would prevent a chain of around 22,000 to 50,000 subsequent infections. Following the ratio between infections and hospitalisations used by the RIVM, the number of prevented hospitalisations would lie between 300 and 680.

The mortality rate of COVID infections in a country depends significantly on the composition ofits population (age, the prevalence of obesity and diabetes). In a meta-analysis of several studies, Brazeau et al. (2020) estimate the mortality rate in high income countries (with a greater concentration of risk groups) to be 1.15% (0.78~1.79%). This is fairly close to the current ratio of 1.06% based on the official statistics for the Netherlands,[765] and at the high end of the bandwidth of 0.5~1.4% for the first wave in European countries, mentioned in a more recent CBS publication (Stoeldraijer et al. 2021). During the second half of the time span from September 2020 – April 2021, the vaccination programme started to gather steam (which started to protect vulnerable groups from the beginning of January); in the estimations below, a mortality rate of 0.5%, at the low end of these estimations, is used. This implies that between 110 and 250 deaths were prevented by the *CoronaMelder.*

So, how do the health benefits of the *CoronaMelder* compare to the estimated costs of the app and the social cost estimate of testing? Since the focus here is on the health benefits due to positive cases detected via the app, the costs of testing these cases should also be included, and a total cost estimate of €48 million is used. Simply looking at the infections prevented, these total costs range from €960 to €2,180 per infection; looking only at the deaths prevented, they are in the order of €190-440,000 per death prevented. At a value of €80,000 per healthy life year lost (Zorginstituut Nederland 2018), these costs per death prevented would equal an average of 2.4~5.5 healthy life years lost. At first sight, these numbers do not look unrealistic. Note that Doti (2021) used a much higher age-adjusted value of statistical life of $4.2 million and Broughel and Kotrous (2021) a value per life saved of around $1 million.

These numbers imply that the social costs associated with the *CoronaMelder* may be offset by the prevented lost value of statistical life, merely on the basis of prevented deaths. A more refined calculation of the expected life years saved by prevented deaths could make this even more precise. The additional social benefits in a more refined calculation would derive from prevented symptomatic short COVID cases with effects in the order of a few days' sick leave, prevented long COVID cases with serious losses in quality of life over several months, and the prevented costs of hospitalisation.

[764] The RIVM estimate was based on 7.5 thousand positive tests triggered by the app, while during the period September-April, there were 11,000 such tests, i.e., 47% more.

[765] 17,695 deaths and 1.67 million infections as per 8 June 2021, both likely to suffer from underreporting.

8.4.2 Costs and benefits relative to manual contact tracing

Lastly, a brief comparison of costs and benefits is made relative to those of manual contact tracing. In Ebbers et al. (2021, p. 22), 1,377 test applications were attributed to manual contact tracing (following the same logic of which 139,000 tests are attributed to the *CoronaMelder).* A larger share of 18% or 226,000 of these tests turned out positive. Using the same estimate for the social costs per test as for the app (€257), this translates to a social cost of €354 million of testing triggered by manual contact tracing.

To complete the picture, an estimate of the costs of manual contact tracing is required. In a newspaper interview, GGD director Sjaak de Gouw estimated the time required for proper contact tracing at around 8 hours, but due to the high numbers of those infected, investing so much time is often not possible.[766] Assuming an average of 2 hours of contact tracing for each infection at an hourly cost of €24 including overheads, the cost of manual contact tracing for the 1.1 million infections in the period September 2020 – April 2021 would be in the order of €54 million. This would bring the full costs of manual contact tracing and the tests it triggered to around €410 million.

Per positive test that manual contact tracing triggers, this corresponds to €1,800. Note that this number is based on a very rough estimate for the number of hours invested in contact tracing and assumes these contacts would not apply for a test without contact tracing.

For the *CoronaMelder* app, this metric this is around €4,400 (11,000 positive tests triggered by the app, at a total social cost of around €48 million). Despite the fact that these numbers are necessarily based on many assumptions, some of which are rather crude, this suggests that the full social costs of detecting infections via the *CoronaMelder* app are higher than via manual contact tracing. This outcome does not so much depend on the costs of developing the app, but rather at the lower percentage of positive tests triggered by the app: 10.4% for the app, versus 18.1% for manual contact tracing. As a result, the social costs of negative tests outweigh the efficiency of the app.

8.5 Conclusions and discussion

This paper developed an economic perspective on the *CononaMelder*, the Dutch contact tracing app launched 10 October 2020 with the aim to assist or supplement public health institutions in tracing the recent contacts of someone testing positive for COVID-19, which may have led to new infections, and to slow down the spread of the virus by urging these contacts to be tested and quarantine until it was clear if they were also infected.

Analysing the incentives for using digital contact tracing apps, it is observed that there are *no personal health benefits for a user of the app*. The app increases the likelihood of early detection of being infected and by doing so, enables one to take action to avoid spreading the virus further. Thus, any potential health benefits fall on the contacts a person would have had (and via them to others), while any potential costs fall on the person installing the app.

This asymmetry remains a fundamental obstacle for large-scale voluntary adoption. Therefore, it remains essential to reduce the actual and the perceived personal costs of using the app to increase its adoption. Particularly in relation to privacy issues, misconceptions about how the app works could be reduced by providing better information. From an economic perspective, even subsidizing app users to compensate them for the positive externalities of installing and using the app could be justified. One way to do this would be a lottery amongst active app users, like the State of Ohio did amongst people who were vaccinated, leading to a substantial increase in the vaccination rate.

[766] https://www.parool.nl/nederland/ggd-baas-over-contactonderzoek-liever-zelf-bellen-omdat-er-schaamte-is~b590d7cb/.

A tentative analysis of the social costs and benefits of the *CoronaMelder* app suggests the benefits balance the costs, even if only looking at life years saved by preventing Corona deaths. Additional social benefits in a more refined calculation would derive from prevented symptomatic short-term COVID cases with effects in the order of a few days' sick leave, prevented long-term COVID cases with serious losses in quality of life over several months, and the prevented costs of hospitalisation.

On top of this, future benefits of the app could be generated if the app contributes to the possibility of rolling back social distancing interventions and the re-opening of society. The latter will increase the number of contacts with people that a person who is positive does not know and therefore, cannot be notified privately or via manual contact tracing.

The accuracy of app notifications – the percentage of tests triggered by the app that turn out positive – is key to its positive contribution to social welfare. This percentage is considerably lower for the app than for tests triggered by manual contact tracing, which suggests it can be efficient as an addition to manual contact tracing, rather than as a substitute for it. This is further underscored by the relatively low adoption rate of the app.

8.6 References

Andreoni, J. (1989). Giving with Impure Altruism: Applications to Charity and Ricardian Equivalence. *Journal of Political Economy, 97-6* (Dec 1989): 1447-1457.

Baarsma, B., E. van den Broek-Altenburg, G. van den Berg, C. Teulings (2021). Langetermijnbelangen worden bij de aanpak van corona veronachtzaamd, *ESB 16 April 2021.*

Brazeau, N.F., R. Verity, S. Jenks et al. (2020). *Report 34: COVID-19 Infection Fatality Ratio: Estimates from Seroprevalence*. Imperial College COVID-19 response team, 29 October 2020.

Broughel, J., M. Kotrous (2021). The benefits of Coronavirus suppression: A cost-benefit analysis of the response to the first wave of COVID-19 in the United States, *Covid Economics 67*, 4 February 2021: 128-171.

Centraal Planbureau (2019). *Decemberraming: Economisch Vooruitzicht 2020.* Den Haag.

Centraal Planbureau (2020). *Juniraming 2020.* Den Haag.

Centraal Planbureau (2021). *Centraal Economisch Plan 2021.* Den Haag.

Doti, J.L. (2021). Benefit-cost analysis of COVID-19 policy intervention at the state and national level, *Covid Economics 67*, 4 February 2021: 94-127.

Ebbers, W., L. Hooft, N. van der Laan, E. Metting (2021). *Evaluatie CoronaMelder. Een overzicht na 9 maanden.* Erasmus University Rotterdam/UMC Utrecht/Tilburg University/Rijksuniversiteit Groningen.

Ferretti, L. C. Wymant, M. Kendall et al. (2020). Quantifying SARS-CoV-2 transmission suggests epidemic control with digital contact tracing. *Science 368*, 619. (8 May 2020).

Giessen, A. van, A. de Wit, C. van den Brink et al. (2020). *Impact van de eerste COVID-19 golf op de reguliere zorg en gezondheid. Inventarisatie van de omvang van het probleem en eerste schatting van gezondheidseffecten*, RIVM-rapport 2020-0183. Bilthoven.

Rehse, D., F. Tremöhlen (2020). Fostering Participation in Digital Public Health Interventions: The Case of Digital Contact Tracing (2020). *ZEW - Centre for European Economic Research Discussion Paper No. 20-076*, Available at SSRN: https://ssrn.com/abstract=3761710.

Stoeldraijer, L., T. Traag, C. Harmsen (2021). *Oversterfte tijdens eerste golf corona-epidemie bijna dubbel zo hoog als tijdens griepepidemie*, CBS 21 May 2021.

Teulings, C.N. (2021). School-closure is counterproductive and self-defeating, *Covid Economics 69,* 18 February 2021: 166-175.

Zorginstituut Nederland (2018). *Ziektelast in de praktijk. De theorie en praktijk van het berekenen van ziektelast bij pakketbeoordelingen*.

9 A monitoring framework for the societal implications of technological solutions

9.1 Creating a monitoring framework for the societal implications of the CoronaMelder and other technological solutions

The monitoring tool that we developed as part of the project consisted of three consecutive survey waves among a representative sample of the Dutch population. In the following, the surveys (codebook) as well as a short presentation of the main outcomes are given. The monitoring tool was designed to improve our understanding of the attitudes and motivations of users to install or not install the CoronaMelder, and signal any individual or broader societal concerns emerging. More specifically, the aim of the tool is first, to observe societal attitudes towards such technologies, concerns related to their implementation, levels of trust, experiences and behavioral intentions, and second to identify groups (e.g. based on demographics, health status or literacy levels) that differ in their degree of acceptance of such technologies, or that are excluded or disproportionality affected.

The framework in form of a three-wave longitudinal survey instrument (administered between June 2020 and January 2021) enabled us to monitor the implementation of the CoronaMelder and a number of other digital measures. With additional support of the SIDN funds, the framework could be extended with two further data collections allowing us to monitor the implementation over the course of a year. The insights from the monitor were shared with ZonMw and the ministries, discussed in a number of media contributions (See appendix 2) and informed our research.

9.2 Survey Wave 1: Main findings and methodology

9.2.1 Summary of the research

9.2.1.1 Purpose

Digital technologies can be part of solutions to societal crises. In fact, technological solutions are important in strategies to manage the current pandemic. These technologies range from medical data mining, use of cell phone location data to monitoring population movements and compliance, self-reporting and -diagnosis applications, and apps for contact tracking and tracing (Bullock, Luccioni, Hoffmann Pham, Sin Nga Lam, & Luengo-Oroz, 2020).

The aim of this research is first, to observe societal attitudes towards such technologies, concerns related to their implementation, levels of trust, experiences and behavioral intentions, and second to identify groups (e.g. based on demographics, health status or literacy levels) that differ in their degree of acceptance of such technologies, or that are excluded or disproportionality affected.

9.2.1.2 Sample

This report presents preliminary findings from the first wave of a longitudinal survey carried out by I&O. In total, 2274 Dutch respondents from all regions of the Netherlands took part in the survey (response rate 49%). A closer inspection shows:

1. 49% females
2. Average age of 52 (SD = 16, range: 18-100)
3. 22% finished lower level of education, 39% finished medium level of education, while 39% finished higher level of education

9.2.2 Main findings

1. While awareness of the contact tracing app is high (93% of respondents have heard about the app), preliminary analyses show confusion about the working of the proposed CoronaMelder app. Motivation to install such an app (after receiving a short explanation of how the app works) is rather low and does not substantially increase (or decrease) with age.

2. Respondents report a number of concerns about both short- and long-term consequences of using the contact tracing app. Particularly long-term consequences, such as negative consequences for vulnerable groups, contribute to lower motivation to install such an app. Short-term consequence, such as being denied access to certain public spaces, do not play a significant role in one's willingness to use the app.

3. Regarding health of respondents and motivation to install the contact tracing app, perceived health status is of importance for particularly older respondents. For respondents 60 years old and older, the worse their perceived health, the more motivated they are to install the app. For these respondents perceived susceptibility to COVID-19 also plays a stronger role in predicting their motivation to install the app (while perceived severity is of less importance for younger respondents).

4. Regarding social norms, descriptive norms (i.e., perception that installing the app is common) do not play a role in motivation to install the contact tracing app. Injunctive norms (i.e., the perceived approval of installing the app by others) predicts motivation to install the app for younger respondents (under 49). For older respondents, we find no relation between norms and motivation to install the app.

5. Trust is an important predictor for motivation to install the contact tracing app. Specifically, trust in government and risk perceptions about sharing data with the government significantly and substantially predict motivation to install the contact tracing app. While individuals with higher trust are more motivated to install the app, perceived risk lowers this motivation. On the contrary, trust in platforms such as Google and risk perceptions about sharing data with such platforms significantly, but less substantially contribute to motivation to install the contact tracing app.

6. Regarding the aim of the app, respondents see it as acceptable to share the data from it with public health institutions for the purpose of helping the society and improving public health. Sharing for different purposes (e.g., with employers) is seen as not acceptable. This shows the rejection of so-called context creep (using information in a context different than the original context of the app).

9.2.3 Methodology

9.2.3.1 Sample characteristics

The target population for this study consisted of people living in the Netherlands above the age of 18. The sample is representative for the Dutch population. The online survey ran from July 6 to July 21 (15 da ys) and was distributed by I&O. The total sample size was N = 2274 (response rate 49%). Below, a detailed breakdown is offered from the sample:

- 49% were women, and 51% men.
- 19% was 18-34 years old, 20% 35-49 years old, 34% 50-64, and 27% 55+ years old
- 22% had a lower education level, 39% medium education level, and 39% higher education level

Age was measured as a continuous variable, but was re-coded into three groups. The variable educational level was re-coded as well to form a smaller set of options (low-moderate-high). The initial education variable consisted of seven levels of Dutch education system.

9.2.3.2 Measures

Measures for **awareness of the contact tracing app & motivation** to install it, as well as **motivation to use different technologies**, were constructed by the researchers.

Perceived health status was measured using validated instrument from Jansen-Kosterink et al. (2020). The variable consisted of three items measured on a 7-point scale ranging from strongly disagree to strongly agree. An example item was: "I am sick more often than other people of the same age and gender".

Privacy concerns were measured using validated instrument from Baek and Morimoto (2012) and Allen (2013) consisting of seven items. To measure **concerns about short- and long-term consequences**, we constructed a variable with five items. All concern variables were measured on a 7-point scale ranging from strongly disagree to strongly agree. An example item was: "I am concerned that data collected through the contact tracing app will not be stored securely".

To measure **social norms**, we used validated instrument from Kaushik and Rahman (2015). We used 5 items (two for descriptive norm and three for injunctive norm) and asked them on a 7-point scale ranging from strongly disagree to strongly agree. An example item was: "People who are important to me think I should use the contact tracing app".

Perceived severity & susceptibility to COVID-19 was measured following the instrument developed by the RIVM. The variables consisted of each two questions answered on a 7-point scale. An example question was: "What are the chances that you will become infected with the corona virus in the coming months?".

To measure **digital efficacy**, validated instrument by Eastin and LaRose (2000) was used. The variable consists of 8 items, and are measured on a 7-point scale ranging from no confidence to a lot of confidence. An example item was: "How much confidence do you have that you can use apps on mobile devices?".

To measure **trust perceptions & risk perceptions** regarding the government and platforms, we used validated instruments from Malhotra et al. (2004). Both variables consist of 5 items, and are measured on a 7-point scale ranging from strongly disagree to strongly agree. An example item was: "The government is fair when it comes to the use of my personal data."

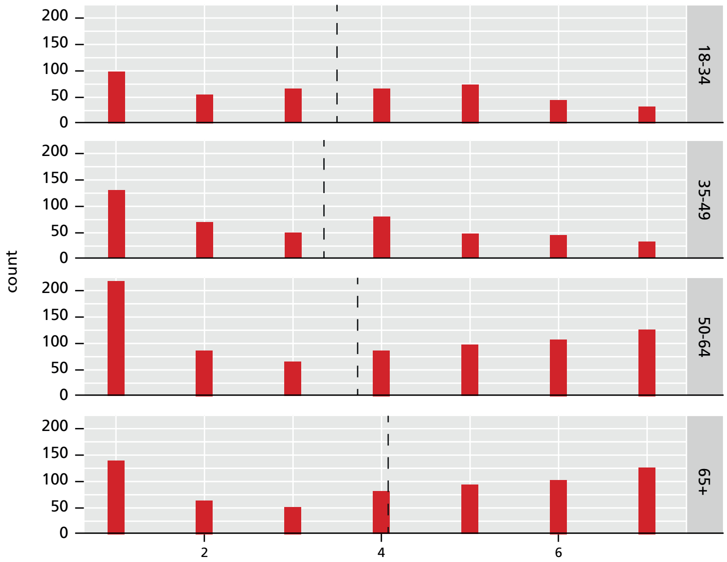
All latent variables were found to be reliable constructs (Cronbach's alpha of at least .7).

9.2.4 Monitoring framework

9.2.4.1 Awareness of the contact tracing app and motivation to install it

- 93% of respondents were aware of the contact tracing app.
- Almost half of respondents were rather not motivated to install the app (1046 (46%) answered that they are at least rather not motivated, 302 (13%) were neutral)
- Age is weakly positively correlated with the motivation to install the app (Pearson's r = .10, $p < .01$).

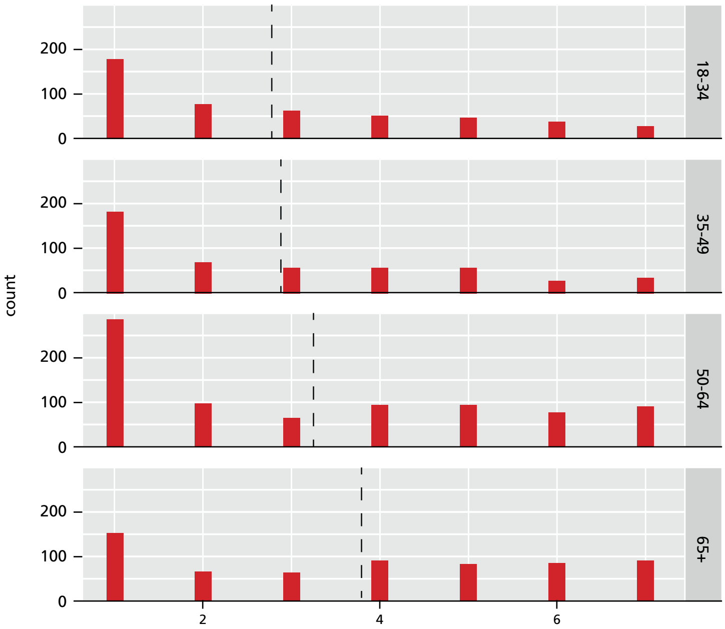
Figure 1. Motivation to install app



9.2.4.2 *Motivation to use different technologies*

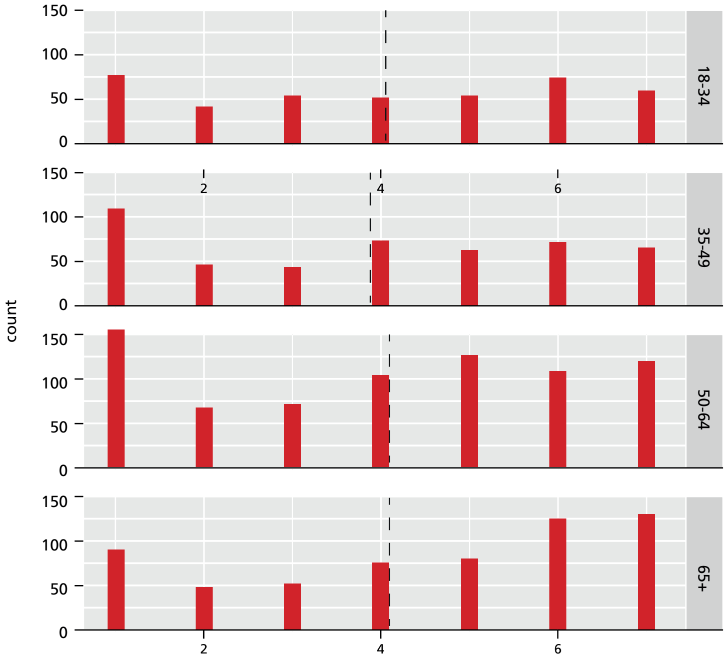
1. Sharing mobile phone data for obligatory quarantine
   - Most respondents were rather not motivated to share mobile phone data for obligatory quarantine (1292 answered that they are at least rather not motivated, 275 are neutral)
   - Age is moderately positively correlated with the motivation to share mobile phone data for obligatory quarantine (Pearson's r = .18, $p < .01$)

Figure 2. Motivation to share data for quarantine



2. Having temperature measures e.g., when entering a shop
   - Almost half of respondents were rather not motivated to have their temperature measured when e.g., entering buildings (1109 (49%) answered that they are at least rather motivated, 313 (14%) are neutral)
   - Age is weakly positively correlated with the motivation to have temperature measured when e.g., entering buildings (Pearson's r = .09, $p < .01$).

Figure 3. Motivation to have temperature measured

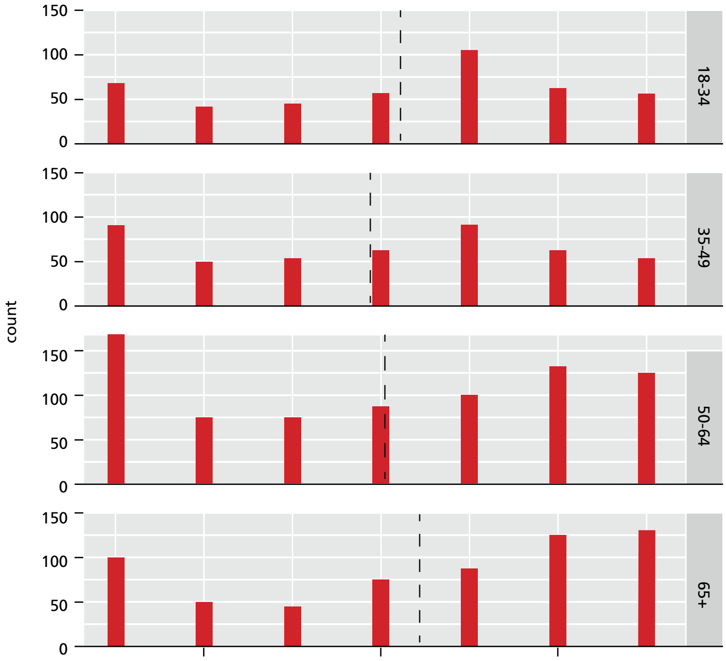


3. Motivation to install an app that proves being healthy
   - Almost half of respondents were not motivated to install an app that proves that they are healthy (1086 (48%) answered that they are at least rather not motivated, 302 (13%) are neutral)
   - Age is weakly positively correlated with the motivation to install an app that proves being healthy (Pearson’s r = .08, *p* < .01)

4. Using self-diagnosis app

   - Half respondents were motivated to use an diagnosis app (1152 (50%) answered that they are at least rather motivated, 277 (12%) are neutral)
   - Age is weakly positively correlated with the motivation to use a self-diagnosis app (Pearson’s r = .05, *p* < .01).

Figure 4. Motivation to use self-diagnosis app



Motivation to share data via contract tracing apps

- On average, respondents were rather not motivated to share their data via the contact tracing app (*M* = 3.52, *SD* = 2.06)
- Age is positively correlated with motivation to share their data via the contact tracing app (Pearson's r = .12, *p* < .01)

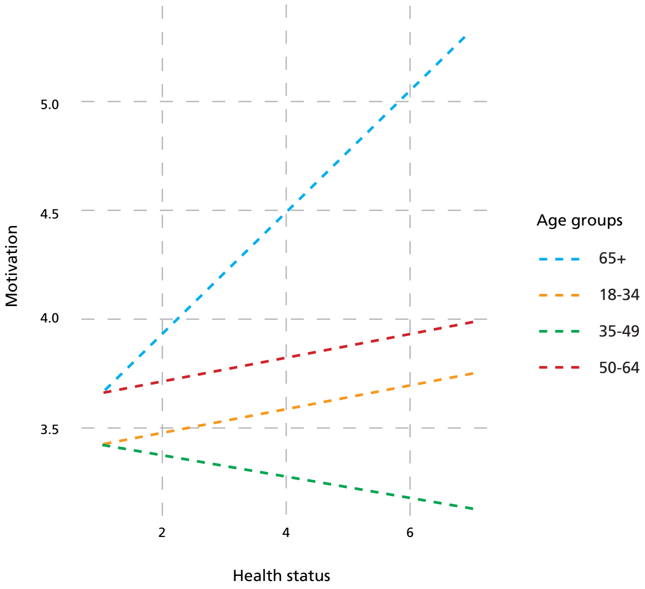
9.2.4.5 Awareness of events related to the crisis

Event	Not heard of at all	Heard of at least a little
First demonstration against corona rules	30% (679)	70% (1595)
Local lockdown in Germany	48% (1090)	52% (1184)
Proposal for the new corona law	49% (1105)	51% (1169)
No corona-related casualties in the Netherlands on June 22nd	63% (1426)	37% (848)
Appathon organized by the Ministry of Health	73% (1673)	26% (601)
Data leak from the RIVM-infectieradar	80% (1818)	20% (456)
Approval for the RIVM to use mobile network data	92% (2089)	8% (185)

9.2.4.6 Perceived health status and motivation to install the app

Overall, perceived health status positively predicts motivation to install the app, *b* = 0.28, *t* = 3.62, *p* < .01. A moderation analysis shows that effect of perceived health status is stronger for older individuals (65+) and weaker for individuals between 35 and 49 years old, R^2 = .02, *F*(7, 2259) = 7.11, *p* < .01.

Figure 5. Relation between health status and motivation to install the app for four age groups.



9.2.4.7 Concerns about consequences of using the app and motivation to install it

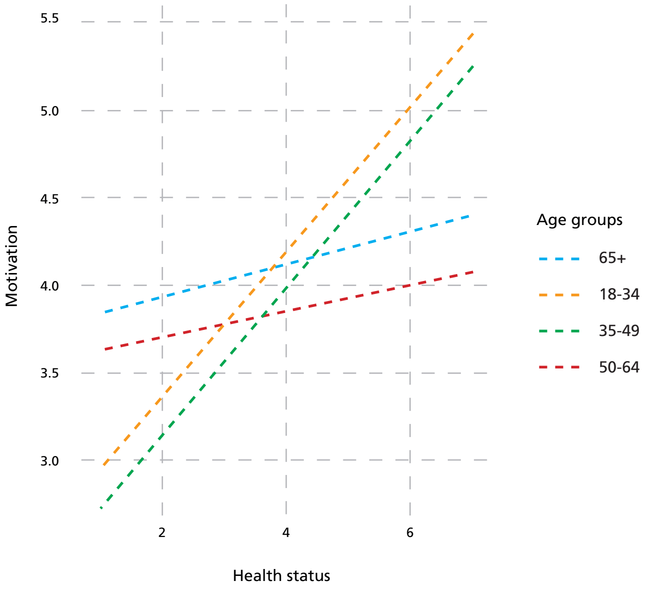
Privacy concerns significantly lowered people's motivation to install the app, *b* = -0.42, *t* = -12.65, *p* <.01. Similarly, concerns about long-term consequences of using the app, such as negative consequences for vulnerable groups, significantly lowered the motivation to install the app, *b* = -0.38, *t* = -10.79, *p* <.01. In contrast, concerns about short-term consequences of using the app, such as being denied access to public space, did not significantly predict motivation to install the app, *b* = .02, *t* = 0.70, *p* = .49, R^2 = .32, *F*(5, 2268) = 219.1, *p* < .01.

9.2.5 Further insights: social norms, concerns and acceptance

9.2.5.1 Social norms and motivation to install the app

Injunctive norms do not predict motivation to install the app for the entire population, *b* = 0.09, *t* = 1.64, *p* = .10. However, moderation analysis shows that injunctive norms do predict motivation to install the app for individuals between 18 and 34 years old, b = 0.32, t = 3.21, p < .01 and for individuals between 35 and 49 years old, b = 0.33, t = 3.47, p < .01, R^2 = .22, *F*(11, 2262) = 60.51, *p* < .01.

Figure 6. Relation between social norms and motivation to install the app for four age groups.

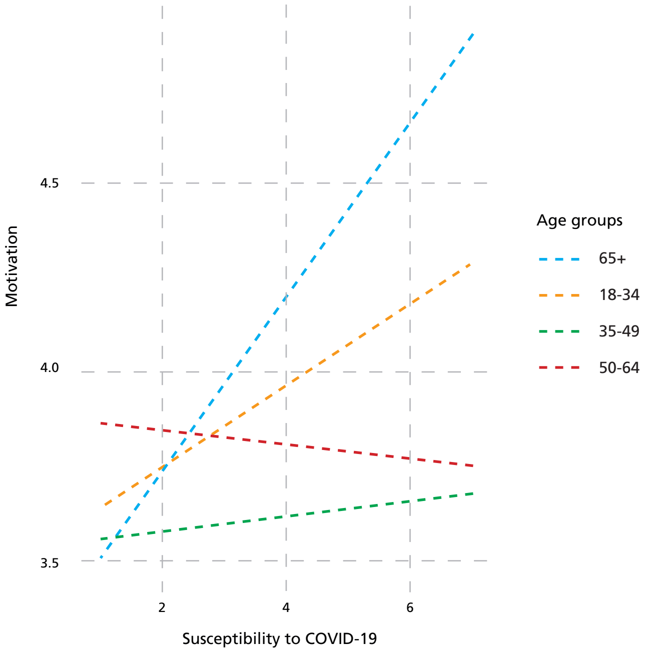


Descriptive norms positively predict motivation to install the app, *b* = 0.61, *t* = 9.66, *p* < .01 and it does not differ per age group, R^2 = .22, *F*(11, 2262) = 60.51, *p* < .01).

9.2.5.2 Susceptibility to and severity of COVID-19

Susceptibility to getting infected significantly predicted motivation to install the app, $b = 0.61$, $t = 9.66$, $p < .01$. Looking at age groups, this relation is stronger for individuals 65 years old and older, $b = -0.25$, $t = -2.55$, $p = .01$, $R^2 = .04$, $F(15, 2258) = 6.27$, $p < .01$.

Figure 7. Relation between perceived susceptibility to COVID-19 and motivation to install the app for four age groups.



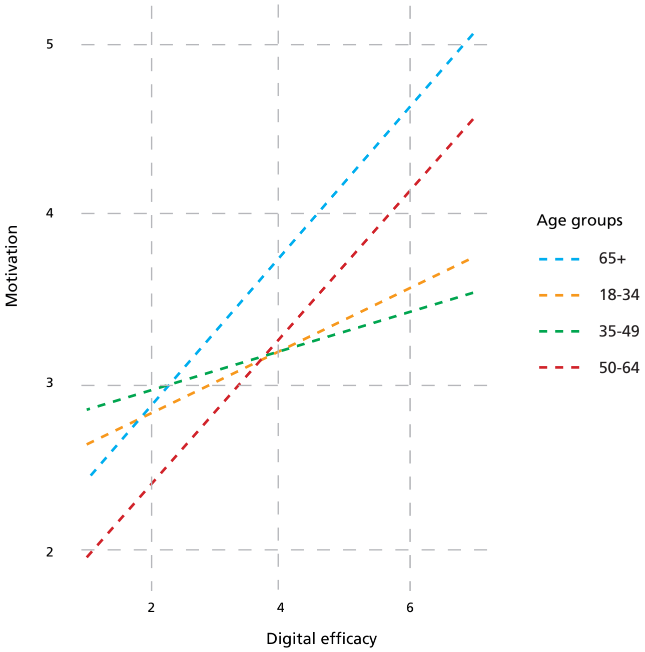
Susceptibility to getting others infected did not significantly predict motivation to install the app, $b = 0.09$, $t = 1.77$, $p = .08$, $R^2 = .04$, $F(15, 2258) = 6.27$, $p < .01$).

Severity of COVID-19 significantly predicted motivation to install the app, $b = 0.34$, $t = 3.08$, $p < .01$ and this relation did not differ per age group, $R^2 = .04$, $F(15, 2258) = 6.27$, $p < .01$).

9.2.5.3 Digital efficacy and motivation to install the app

Digital efficacy significantly predicted motivation to install the app, *b* = 0.44, *t* = 6.83, *p* < .01. Looking at age groups, compared to 65+ individuals, for younger individuals the impact of digital efficacy is less strong, 18-34: *b* = -0.26, *t* = -2.43, *p* = .02; 35-49: *b* = -0.33, *t* = -3.14, *p* < .01, R^2 = .06, *F*(7, 2266) = 20.46, *p* < .01).

Figure 8. Relation between digital efficacy and motivation to install the app for four age groups.



9.2.5.4 Beliefs about government and motivation to install the app

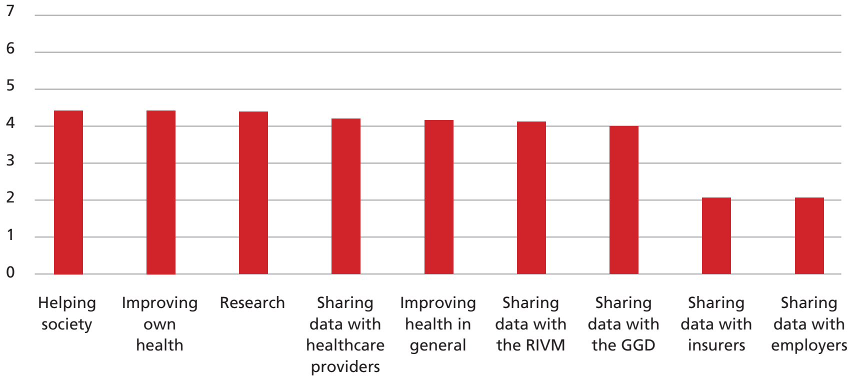
Trust in the government (*b* = 0.46, *t* = 4.63, *p* < .01) and risk perceptions about sharing data with the government (*b* = -0.41, *t* = -3.47, *p* < .01) significantly predicted motivation to install the app. The relation did not differ with age, R^2 = .32, *F*(5, 2268) = 209.9, *p* < .01.

9.2.5.5 Beliefs about platforms and motivation to install the app

Trust in platforms such as Google (b = 0.30, t = 2.17, p < .01), and risk perceptions about sharing data with such platforms (b = -0.41., t = -2.82, p < .01) significantly predicted motivation to install the app. The relation did not differ with age, R^2 = .06, F(5, 2268) = 32.23, p < .01.

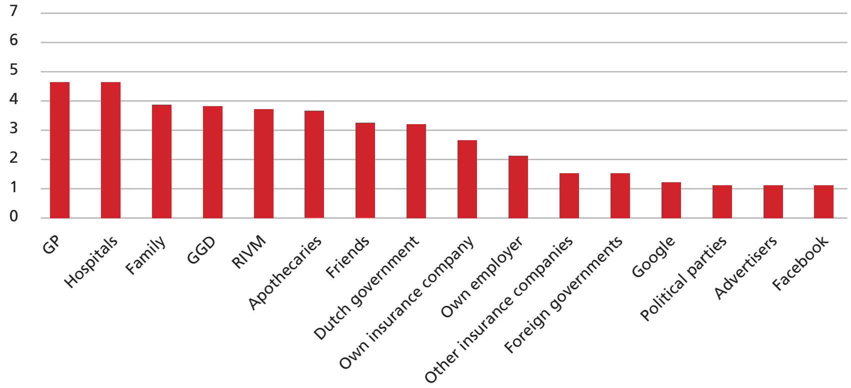
9.2.5.6 Aims of the app and acceptance of it

Figure 9. Average acceptance



9.2.5.7 Acceptance of different parties having access to the data collected by the app

Figure 9. Average acceptance



9.2.6 Discussion

Overall, understanding of the functioning app as well as the motivation to install the contact tracing app are rather low. This also means that if the government hopes to reach broad adoption, it will need to step up its efforts to explain the app and communicate why people should install it. In so doing, it is important to notice that different societal groups are motivated by different arguments to install the app. In particular, among the group of 60+, health related concerns play a more important role. Thus, when communicating about the app to this groups, it is critical to explain how the app can help to avoiding contracting the virus. To the contrary, among the group of under 50, social pressure seems to be a more important factor to install the app, raising potential red flags about the voluntariness of installing the app in that age group that should be further researched.

Remarkable is the fact that concerns about the long-term consequences and in particular the impact on potential vulnerable groups as well as privacy concerns influence the motivation to install the app in all age groups. This finding highlights the importance of considering also long-term implications of technological solutions, such as the app, as well as communicating about the fact that the government is aware of, and prepared to act to protect against adverse impact on privacy and long-term negative consequences for particularly vulnerable groups or function creep. Findings like these lend further weight to the importance of adopting formal legislation, such as the *Tijdelijke wet notificatieapplicatie COVID-19.*

In terms of democratic legitimatisation of government's decisions, it is remarkable to constat that the majority of Dutch citizens are not aware of the Appathon – a measure that has been designed with the explicit goal of enhancing transparency and including the population into the design process of the contact tracing app. Whereas the Dutch approach has been celebrated throughout Europe for its transparency, the findings from this survey also raise questions regarding the effectiveness of that particular measure, and highlight the need for even clearer communication vis-a-vis the general population.

9.2.7 References

Allen, A. L. (2013). An ethical duty to protect one's own information privacy? *Faculty Scholarship at Penn Law*. 451. Retrieved from: https://scholarship.law.upenn.edu/faculty_scholarship/451

Baek, T. H., & Morimoto, M. (2012). Stay away from me. *Journal of advertising, 41*(1), 59-76.

Eastin, M. S., & LaRose, R. (2000). Internet self-efficacy and the psychology of the digital divide. *Journal of Computer-Mediated Communication, 6*(1).

Jansen-Kosterink, S. M., Hurmuz, M., den Ouden, M., & van Velsen, L. (2020). Predictors to use mobile apps for monitoring COVID-19 symptoms and contact tracing: A survey among Dutch citizens. *medRxiv*.

Kaushik, A. K., & Rahman, Z. (2015). An alternative model of self-service retail technology adoption. *Journal of Services Marketing.*

Luccioni, A., Bullock, J., Pham, K. H., Lam, C. S. N., & Luengo-Oroz, M. (2020). Considerations, Good Practices, Risks and Pitfalls in Developing AI Solutions Against COVID-19. *arXiv preprint arXiv:2008.09043*.

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research, 15*(4), 336-355.

9.3 Survey Wave 2: Main findings and methodology

9.3.1 Summary of the research

9.3.1.1 Purpose

Digital technologies can be part of solutions to societal crises. In fact, technological solutions can, under certain conditions, be important in strategies to manage the current pandemic. These technologies range from medical data mining, use of cell phone location data to monitoring population movements and compliance, self-reporting and -diagnosis applications, and apps for contact tracking and tracing (Bullock et al., 2020).

The aim of this research is first, to observe how societal attitudes towards such technologies, concerns related to their implementation, levels of trust, experiences and behavioral intentions develop over time, and second to identify groups (e.g. based on demographics, health status or literacy levels) that differ in their degree of acceptance of such technologies, or that are excluded or disproportionality affected.

9.3.1.2 Sample

This report presents preliminary findings from the first two waves of a longitudinal survey carried out by I&O. In total, 1848 Dutch respondents from all regions of the Netherlands took part in both waves of the survey (drop-out rate of 18%). A closer inspection shows:

1. 47% females
2. Average age of 54 (SD = 16, range: 18-90)
3. 22% finished lower level of education, 40% finished medium level of education, while 38% finished higher level of education.

9.3.2 Main findings

1. Awareness of the contact tracing app remains at the same high level. At the same time, acceptance of the app as well as the motivation to install it have slightly increased over time. Respondents are also slightly more willing to share their data via the contact tracing app.

2. Awareness of the use of telecom data is rather low – only 68% of respondents are aware of the role telecom data plays. At the same time, the acceptance of this measure has moderately increased. The same applies to motivation to actively allow the government to use telecom data if asked – this motivation is slightly higher than in July.

3. 21% of respondents have installed the contact tracing app in October. The respondents that have installed the app are in general positive about it. Regarding interactions with the app, respondents who have installed the app are rather willing to share information about infection and do not intend to misuse it. However, respondents who have not installed the app are more likely to withhold information about infection if they were to install the app. They are also more likely to misuse the app if they were to install it.

4. In the previous report, the important role of social norms (descriptive norms. i.e., perception that installing the app is common, and injunctive norms. i.e., the perceived approval of installing the app by others) for motivation to install the contact tracing app was shown. This part further explores this role; the findings show that in particular, perceptions about family and partner (perceptions what they expect one to do and what they do themselves) are important drivers of motivation to install the app.

   Regarding actually having installed the app, injunctive and descriptive norms are both related to the behavior with descriptive norms being stronger related. Similarly to intentions, perceptions about expectations and behavior of family and partner play the biggest role. Here however, the negative impact of perceived expectations of the employer is stronger (when one believes that their employer expects them to install the app, their odds to do so are lower).

5. In the previous report, trust was concluded to be an important predictor for motivation to install the contact tracing app. Further investigations show that while trusting beliefs in the government and risk perceptions of data sharing with the government are related to intention to install the app and actual installation behavior and trusting beliefs in digital media tech companies and risk perceptions of data sharing with these companies do not play a role, the risks perceived from the collaboration between the government and the digital media tech companies are important for both intentions and behavior.

9.3.3 Methodology

9.3.3.1 Sample characteristics

The target population for this study consisted of people living in The Netherlands above the age of 18. The sample is representative for the Dutch population. The online survey was distributed by the research company I&O. The first wave of the survey ran from July 6 to July 21 (15 days) and the second wave from October 9 till October 15 (6 days). The total sample size was N = 2274 at wave 1 and N = 1848 at wave 2 (drop-out rate of 18%). Below, a detailed breakdown is offered from the sample at wave 2:

- 47% were women, and 53% men.
- 17% was 18-34 years old, 19% 35-49 years old, 35% 50-64, and 29% 65+ years old
- 22% had a lower education level, 40% medium education level, and 38% higher education level

The variable educational level was re-coded to form a smaller set of options (low-moderate-high). The initial education variable consisted of seven levels of Dutch education system.

9.3.3.2 Measures

Measures for **awareness of the contact tracing app & motivation** to install it, as well as **motivation to use different technologies**, were constructed by the researchers. They were measured in both waves.

Emotional states were measured through a validated scale developed by Watson, Clark & Tellegen (1988) consisting of 7 items measured on a 7-point scale. The respondents were asked to what extent the experienced seven different states when having the contact tracing app installed including feeling troubled, guilty, proud, alert, ashamed, nervous and scared. The scores on negative states were averaged to create a scale. One positive state (pride) was analyzed separately.

Information disclosure and withdrawal intention was measured by adopting a scale developed by Dienlin and Metzger (2016). The scale consisted of 3 items measuring how likely the respondent is to take different actions. One item measured disclosure intention ("If you are tested positive, to report a positive result of the corona test?") and two items measured withdrawal intention ("Turn off Bluetooth so that the app cannot exchange data?" and "Switch off your telephone in public areas (e.g., in a shop)?"). Two scales were used, one for disclosure and another for withdrawal intention.

To measure **social norms**, we adopted validated instrument from Kaushik and Rahman (2015). We used 9 items (four for descriptive norm and five for injunctive norm) and asked them on a 7-point scale ranging from strongly disagree to strongly agree. Each item focused on a different potential reference for social norms, including friends, family, partner, people in one's direct environment and employer. An example item was: "My direct family thinks I should use the contact tracing app".

To measure **trust perceptions & risk perceptions** regarding the government and platforms, we used validated instruments from Malhotra et al. (2004). Both variables consist of 5 items, and are measured on a 7-point scale ranging from strongly disagree to strongly agree. An example item was: "The government is fair when it comes to the use of my personal data."

Additionally, the risk perception scale was adopted to measure risk perceived due to cooperation between the government and platforms. The scale was self-constructed building on the risk perceptions measure by Malhotra et al. (2004).

All latent variables were found to be reliable constructs (Cronbach's alpha of at least .7).

9.3.4 Monitoring framework

9.3.4.1 Contact tracing app: awareness, acceptance and motivations

Regarding awareness, in July, 93% of respondents were aware of the contact tracing app. This did not change significantly over time (in October, 94% are aware of it, $F(1,1847) = 3.54$, $p = .06$).

Looking at acceptance of the contact tracing app, they have become slightly more acceptable over time ($M_{W1} = 4.33$, $SD_{W1} = 2.13$; $M_{W2} = 4.89$, $SD_{W2} = 2.14$, $F(1,1847) = 182,54$, $p < .01$).

Regarding motivation to install the contact tracing app, in July, almost half of respondents were rather not motivated to install it (46% answered that they wee at least rather not motivated, 13% were neutral). This motivation increased over time very slightly – in October, 45% answered that they are at least rather not motivated, 21% were neutral; $M_{W1} = 3.71$, $SD_{W1} = 2.15$; $M_{W2} = 3.82$, $SD_{W2} = 2.23$, $F(1,1847) = 182,54$, $p < .01$ $F(1,1847) = 10.41$, $p < .01$).

Finally, regarding the motivation to share information via the contact tracing app, it has slightly increased over time ($M_{W1} = 3.52$, $SD_{W1} = 2.06$; $M_{W2} = 3.98$, $SD_{W2} = 2.07$, $F(1,1847) = 153.114$, $p < .01$).

Telecom data: awareness, acceptance and motivations

Regarding awareness, in October, 68% of respondents were aware of the use of telecommunications data by the government.

Looking at acceptance of the use of telecommunications data, it has become more acceptable over time ($M_{W1} = 3.58$, $SD_{W1} = 2.19$; $M_{W2} = 4.29$, $SD_{W2} = 2.27$, $F(1,1847) = 197.25$, $p < .01$).

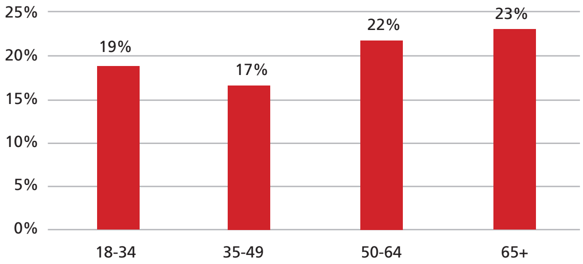
Regarding motivation to allow the government access to telecommunications data (if asked for consent), in July, most respondents were not motivated to do so (57% answered that they are at least rather not motivated, 12% were neutral). This motivation slightly increased over time– in October, 46% answered that they are at least rather not motivated, 14%% were neutral; M_{W1} = 3.23, SD_{W1} = 2.12; M_{W2} = 3.75, SD_{W2} = 2.23, $F(1,1847) = 112.25$, $p < .01$).

9.3.5 Experiences with the contact tracing app

9.3.5.1 Installation of the app

In total, 21% of respondents have installed the contact tracing app CoronaMelder. The graph below presents installation rates for different age categories: age and installation and weakly correlated (*Pearson's r* = .05, $t(1716) = 1.96$, $p = .05$).

Figure 10. Installation rate



Among the ones who have installed the app, 90% have actually activated (by turning and keeping Bluetooth on) (SD=0.3).

9.3.5.2 Feelings and attitudes

Regarding negative emotional states, respondents who have installed the app show slightly less negative emotional states stemming from using the app (M = 1.83) than respondents who did not install it (M = 2.32), $t(777) = 8.67$, $p < .01$.

Regarding pride, respondents who have installed the app show more pride (M = 2.62) than respondents who did not install it (M = 1.92), $t(481) = -7.04$, $p < .01$.

The respondents that have installed the app are in general positive about it (M=5.74, SD=1.44). This attitude is not related to respondents' age or gender (F (3,350) = 1.05, p = .37).

9.3.5.3 Information disclosure and withdrawal intention

The respondents who have installed the app are more willing to disclose infection (M = 6.75, SD = 0.7) than respondents who have not installed the app (when asked to imagine that they would install it, M = 1.33, SD = 0.77), $t(516) = -120.65$, $p < .01$.

Along these lines, the respondents who have installed the app are less likely to withhold information from the app by turning it off or deactivating it (M = 1.44, SD = 0.49) than respondents who have not installed the app (when asked to imagine that they would install it, M = 2.03, SD = 0.98), $t(399) = 11.06$, $p < .01$.

9.3.6 Further insights: social norms and trust

9.3.6.1 Impact of social norms on intentions and behavior

In the first wave of the survey, general measures of injunctive and descriptive norms were included. The results showed that injunctive norms did not predict motivation to install the contact tracing app for the entire population, but only for individuals between 18 and 49 years old. Descriptive norms positively predicted motivation to install the app. In general, norms were as expected important predictors of the motivation. Therefore, second wave included more detailed measurements of social norms.

Looking at the impact of these norms on motivation to install the app, both injunctive and descriptive norms significantly positively impact the motivation. Impact of descriptive norms is stronger. Together with age, gender and level of education and controlling for motivation at wave 1, they explain more than 60% of variation in the motivation. Descriptive norms have stronger impact on motivation than injunctive norms (see Table 1).

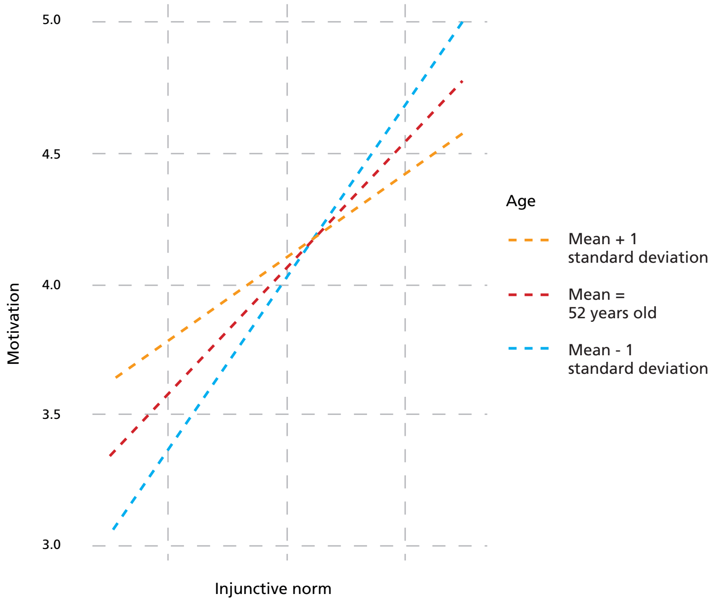
Replication of the interaction with age confirms that injunctive norms are stronger related to motivation to install the app among younger respondents (see Figure 1), while impact of descriptive norms does not differ with age.

Table 1. Predictors of motivation to install the app

	β	SE	t	p
Motivation at wave 1	.44	.02	23.34	<.01
Injunctive norms	.24	.04	6.10	<.01
Descriptive norms	.44	.04	11.44	<.01
Age	.01	.002	3.71	<.01
Gender	.15	.07	2.27	.02
Level of education	.04	.02	1.52	.11

F(6, 1557) = 473.1, *p* < .01, R^2 = .64
Significant predictors are marked in bold

Figure 11. Relation between injunctive norms and motivation to install the app fdepending on age.



To gain further insights into how norms impact individual motivations, an analysis was conducted for different sources of the norms. This analysis shows that in particular, perceptions about family and partner are important for both perceptions what others expect one to do and what they do themselves (see Table 2).

Table 2. Predictors of motivation to install the app

	β	*SE*	*t*	*p*
Motivation at wave 1	.42	.02	22.35	<.01
Injunctive norm - friends	.003	.05	0.07	.94
Injunctive norm – family	.17	.05	3.54	<.01
Injunctive norm – partner	.16	.04	4.27	<.01
Injunctive norm – employer	-.05	.03	-1.89	.06
Injunctive norm – others	-.04	.05	-0.91	.36
Descriptive norms – friends	.07	.05	1.44	.15
Descriptive norms – family	.10	.04	2.37	.02
Descriptive norms – partner	.13	.03	4.15	<.01
Descriptive norms – others	.10	.05	2.16	.03
Age	.006	.002	3.71	<.01
Gender	.17	.07	2.27	.01
Level of education	.04	.02	1.52	.11

F(13, 1550) = 228.4, *p* < .01, R^2 = .65
Significant predictors are marked in bold, marginally significant predictors are marked in italics

Looking at actual installations of the contact tracing app in October, similar relations can be concluded. Both injunctive and descriptive norms are related to the behavior with descriptive norms being stronger related (see Table 3). Again, perceptions about expectations and behavior of family and partner play the biggest role. Here however, the negative impact of perceived expectations of the employer is stronger (when one believes that their employer expects them to install the app, their odds to do so are lower, see Table 4).

Table 3. Predictors of installation behavior

	b	SE	z	p	Odds
Injunctive norms	0.16	0.08	2.03	.04	1.17
Descriptive norms	0.63	0.08	7.57	<.01	1.88
Age	-0.01	0.01	-1.47	.14	0.99
Gender	-0.22	0.15	-1.50	.13	0.80
Level of education	-0.02	0.05	-0.37	.71	0.98

χ2 (5) = 272.19, *p* < .01, *pseudo* R^2 = .19
Significant predictors are marked in bold

Table 4. Predictors of installation behavior

	b	SE	z	p	Odds
Injunctive norm - friends	0.11	0.11	1.03	.30	1.12
Injunctive norm – family	0.19	0.10	1.87	.06	1.21
Injunctive norm – partner	0.13	0.08	1.66	.10	1.14
Injunctive norm – employer	-0.15	0.05	-3.03	<.01	0.85
Injunctive norm – others	-0.08	0.10	-0.81	.42	0.93
Descriptive norms – friends	0.06	0.10	0.54	.59	1.06
Descriptive norms – family	0.18	0.09	1.87	.06	1.19
Descriptive norms – partner	0.33	0.07	4.77	<.01	1.38
Descriptive norms – others	-0.05	0.10	-0.52	.60	0.95
Age	-0.01	0.01	-2.25	.02	0.99
Gender	-0.19	0.15	-1.25	.21	0.82
Level of education	-0.03	0.05	-0.55	.58	0.97

χ2 (12) = 318.42, *p* < .01, *pseudo* R^2 = .22
Significant predictors are marked in bold, marginally significant predictors are marked in italics

9.3.6.2 Impact of trust on intentions and behavior

In the first wave of the survey, measures of trusting beliefs in the government and digital media technology as well as risk perceptions of sharing data with these instances were included. Trust in the government and risk perceptions about sharing data with the significantly predicted motivation to install the contact tracing app, while app trust in digital media technology such as Google, and risk perceptions about sharing data with such companies only weakly predicted motivation to install the app. To further explore this relation, second wave included a more general measure of trust in the government as well as risk perceptions of the cooperation between the government and the digital media tech companies such as Google and Apple.

Regarding motivation to install the contact tracing app, trusting beliefs in government significantly increase it. Trusting beliefs in digital media tech companies decrease the motivation, but this relation is only marginally significant. Regarding risk perceptions, risk perceptions about data sharing with the government and risk perceptions of the collaboration between digital media tech companies and the government significantly decrease the motivation. Together with motivation level at wave 1, age, gender and level of education, these factors explain 56% of variation in motivation to install the app at wave 2 (see Table 5).

Table 5. Predictors of motivation to install the app

	β	SE	t	p
Motivation at wave 1	.54	.02	28.56	<.01
Trust in the government	-.05	.04	-1.27	.20
Trusting beliefs in the government	.29	.04	7.09	<.01
Risk perceptions of data sharing with government	-.13	.04	-3.28	<.01
Trusting beliefs in digital media tech	-.07	.04	-1.92	.06
Risk perceptions of data sharing with digital media tech	.002	.04	0.06	.95
Risk perception of the cooperation	-.18	.04	-4.75	<.01
Age	.01	.002	5.52	<.01
Gender	-.07	.07	-1.00	.32
Level of education	.05	.03	2.03	.04

$F(10, 1837) = 234.2$, $p < .01$, $R^2 = .56$
Significant predictors are marked in bold, marginally significant predictors are marked in italics

Regarding relation to actual installation behavior, trusting beliefs in the government and perceptions about risk of sharing data with the government as well as of working together with tech companies impact the behavior. Trusting beliefs in digital media tech companies and other risk perceptions are not significantly related to the behavior (see Table 6).

Table 6. Predictors of installation behavior

	b	SE	z	p	Odds
Trust in the government	-0.14	0.83	-1.71	.09	0.87
Trusting beliefs in the government	0.48	0.08	5.92	<.01	1.61
Risk perceptions of data sharing with government	-0.19	0.07	-2.61	<.01	0.82
Trusting beliefs in digital media tech	-0.13	0.07	-1.79	.07	0.88
Risk perceptions of data sharing with digital media tech	-0.04	0.07	-0.50	.59	0.96
Risk perception of the cooperation	-0.34	0.07	-4.79	<.01	0.71
Age	0.003	0.004	0.68	.50	1.00
Gender	-0.37	0.13	-2.84	<.01	0.69
Level of education	-0.02	0.05	-0.47	.64	0.98

$\chi 2$ (9) = 263.11, $p < .01$, *pseudo* $R^2 = .15$
Significant predictors are marked in bold, marginally significant predictors are marked in italics

9.3.7 References

Bullock, J., Luccioni, A., Hoffmann Pham, K., Sin Nga Lam, C., & Luengo-Oroz, M. (2020). *Mapping the landscape of Artificial Intelligence applications against COVID-19*. https://arxiv.org/pdf/2003.11336.pdf

Dienlin, T., & Metzger, M. J. (2016). An extended privacy calculus model for SNSs: Analyzing self-disclosure and self-withdrawal in a representative US sample. *Journal of Computer -Mediated Communication, 21*(5), 368-383.

Kaushik, A. K., & Rahman, Z. (2015). An alternative model of self-service retail technology adoption. *Journal of Services Marketing.*

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research, 15*(4), 336-355.

Watson, D., Clark, L. A., & Tellegen, A. (1988). Development and validation of brief measures of positive and negative affect: the PANAS scales*. Journal of personality and social psychology, 54*(6), 1063.

9.4 Survey Wave 3: Main findings and methodology

9.4.1 Summary of the research

9.4.1.1 Purpose

Digital technologies can be part of solutions to societal crises. In fact, technological solutions can, under certain conditions, be important in strategies to manage the current pandemic. These technologies range from medical data mining, use of cell phone location data to monitoring population movements and compliance, self-reporting and -diagnosis applications, and apps for contact tracking and tracing (Bullock et al., 2020).

The aim of this research is first, to observe how societal attitudes towards such technologies, concerns related to their implementation, levels of trust, experiences and behavioral intentions develop over time, and second to identify groups (e.g. based on demographics, health status or literacy levels) that differ in their degree of acceptance of such technologies, or that are excluded or disproportionality affected.

9.4.1.2 Sample

This report presents preliminary findings from the first two waves of a longitudinal survey carried out by I&O. In total, 1610 Dutch respondents from all regions of the Netherlands took part in all three waves of the survey (drop-out rate of 29%). A closer inspection shows:

1. 46% females
2. Average age of 55 (SD = 16, range: 18-90)
3. 22% finished lower level of education, 40% finished medium level of education, while 38% finished higher level of education.

9.4.2 Main findings

1. Awareness of the contact tracing app remains at the same high level. At the same time, acceptance of the app has slightly increased over time. Regarding motivation to install it, it has been dropping among individuals who have not done some. Those who have not installed the app before January are rather not motivated to do so any more and their motivation is dropping with time.

2. Awareness of the use of telecom data has increased – now, 77% of respondents are aware of the role telecom data plays. At the same time, the acceptance of this measure has strongly increased.

3. 21% of respondents have installed the contact tracing app in October and this has increased to 41%. Installation rates significantly increase with age. The respondents that have installed the app are in general positive about it. Regarding interactions with the app, respondents who have installed the app are rather willing to share information about infection and do not intend to misuse it. However, respondents who have not installed the app are rather not motivated to do so any more.

4. In the first report, the crucial role of perceived benefits and costs was concluded. This report further investigates the type of benefits, concerns and costs related to contact tracing technology that individuals perceive. It distinguishes between five types of concerns, three types of benefits and two types of costs. In general, benefits for the social health are the strongest driver of app installation. At the same time, privacy concerns as well as social concerns about how the introduction of such technology will impact the society lower installation rates. In general, societal concerns and benefits are more important drivers and inhibitors of installation compared to perceived benefits and concerns for the individual.

5. This report also zooms into the voluntariness of the app. In general, respondents feel that the decision to use the app is voluntary. Overall, they do not experience pressure from the government nor their employer. However, for individuals with flexible employment, the perception of voluntariness matters. Only if they feel they can voluntarily use the app, the would do so. Further, moral and normative obligation have been investigated. The findings inform us that while respondents do not rather perceive normative obligation to install the app and this obligation does not impact their installation decision, they feel strongly morally obliged to install the app and their moral obligation is an important predictor of their behavior.

9.4.3 Methodology

9.4.3.1 Sample characteristics

The target population for this study consisted of people living in The Netherlands above the age of 18. The sample is representative for the Dutch population. The online survey was distributed by the research company I&O. The first wave of the survey ran from July 6 to July 21 (15 days), the second wave from

October 9 till October 15 (6 days) and the third wave from January 8th till January 19th (11 days). The total sample size was N = 2274 at wave 1, N = 1848 at wave 2 and N = 1610 at wave 3 (drop-out rate of 29%).

Below, a detailed breakdown is offered from the sample at wave 3:

- 46% were women, and 54% men.
- 14% was 18-34 years old, 19% 35-49 years old, 36% 50-64, and 31% 65+ years old
- 22% had a lower education level, 40% medium education level, and 38% higher education level

The variable educational level was re-coded to form a smaller set of options (low-moderate-high). The initial education variable consisted of seven levels of Dutch education system.

9.4.3.2 Measures

Measures for **awareness of the contact tracing app, motivation** to install it and **actual installation behavior**, as well as **motivation to use different technologies**, were constructed by the researchers. They were measured in both waves.

Information disclosure and withdrawal intention was measured by adopting a scale developed by Dienlin and Metzger (2016). The scale consisted of 3 items measuring how likely the respondent is to take different actions. One item measured disclosure intention ("If you are tested positive, to report a positive result of the corona test?") and two items measured withdrawal intention ("Turn off Bluetooth so that the app cannot exchange data?" and "Switch off your telephone in public areas (e.g., in a shop)?"). Two scales were used, one for disclosure and another for withdrawal intention.

Privacy concerns were measured using validated instrument from Baek and Morimoto (2012) and Allen (2013) consisting of seven items. To measure **perceived benefits and concern,** a measure was constructed based on codlings of thought listing included about benefits and concerns related to contact tracing apps included in wave 1.

To measure **voluntariness factors** related to one's employment situation, questions were based on measures used by the CBS in the census. **Moral and normative obligation** was measured by adopting scales developed by Posch et al. (2020)

All latent variables were found to be reliable constructs (Cronbach's alpha of at least .7).

9.4.4 Monitoring framework

9.4.4.1 Contact tracing app: awareness, acceptance and motivations

Regarding awareness, in July and October, respectively 93% and 94% of respondents were aware of the contact tracing app. This increased over time (in January, 97% are aware of it, $F(1,3122) = 10.49$, $p < .001$).

Looking at acceptance of the contact tracing app, they have become moderately more acceptable over time ($M_{W1} = 4.33$, $SD_{W1} = 2.13$; $M_{W2} = 4.89$, $SD_{W2} = 2.14$, $M_{W3} = 5.18$, $SD_{W2} = 2.01$ $F(1,3185) = 181.74$, $p < .001$).

Regarding motivation to install the contact tracing app, among respondents who have not installed the app, the motivation has been decreasing over time. At wave 2, among respondents who did not have the app, most were not motivated to install the app (55.87% answered that they were at least rather not motivated, 18.04% were neutral; M=3.17, SD=1.94). At wave 3, among respondents who did not have the app, most respondents were not motivated to install the app (81.63% answered that they were at least rather not motivated, 7.7% were neutral; M=2.17, SD=1.43; $F(1,1816) = 80.77$, $p < .001$).

9.4.4.2 Telecom data: awareness, acceptance and motivations

Regarding awareness, in October, 68% of respondents were aware of the use of telecommunications data by the government, and this awareness increased to 77% in January ($F(1,1609) = 39.63$, $p < .001$).

Looking at acceptance of the use of telecommunications data, it has become more acceptable over time ($M_{W1} = 3.58$, $SD_{W1} = 2.19$; $M_{W2} = 4.29$, $SD_{W2} = 2.27$, $M_{W2} = 4.98$, $SD_{W2} = 2.07$, $F(1,3172) = 314.05$, $p < .001$).

9.4.5 Experiences with the contact tracing app

9.4.5.1 Installation of the app

In October, 21% of respondents have installed the contact tracing app CoronaMelder. From the respondents who did not have the app in October (N = 1364), 29% has install it between the waves. In January, 41.49% of respondents have installed the Coronamelder; installation rate has strongly increased over time ($F(1,1508) = 392.85$, $p < .001$). Similarly to wave 2, we find a relation between age and installation rates:

Among the ones who have installed the app, 95% have actually activated (by turning and keeping Bluetooth on) (SD=0.21) and 7% is planning to remove the app again.

Among the respondents who did not have the app in January, 46 have tried to install it, but had issues and were thus not able to do so. Main issue was related to the mobile phone owned by the respondent (either too old, not up-to-date software or not enough memory). One respondent mentioned that she/he was not allowed by the employer (their phone was blocked for the app).

9.4.5.2 Feelings and attitudes

The respondents that have installed the app have remained positive about it (M_{W2} = 5.74, SD_{W2} = 1.44, M_{W3} = 5.83, SD_{W3} = 1.96; F(1,297) = 1.16, p = .282).

At the same time, privacy concerns related to the app have significantly decreased (M_{W2} = 4.99, SD_{W2} = 1.69, M_{W3} = 3.87, SD_{W3} = 1.37; F(1,1609) = 782.87, p < .001).

9.4.5.3 Information disclosure and withdrawal intention

Among the respondents who have been using the app since October, the motivation to share positive test result has slightly decreased, but remains high (M_{W2} = 6.75, SD_{W2} = 0.77, M_{W3} = 6.57, SD_{W3} = 1; F(1,297) = 3.66, p = .057).

Along these lines, among the respondents who have been using the app since October, the motivation to withdraw from sharing data with the app (by e.g., turning the app off) has slightly increased (M_{W2} = 1.44, SD_{W2} = 0.98, M_{W3} = 1.75, SD_{W3} = 1.26; F(1,297) = 16.8, p < .001).

9.4.5.4 Intention to follow app's advice

The intention to follow app's advice and stay at home has slightly increased over time (M_{W2} = 5.44, SD_{W2} = 1.70, M_{W3} = 5.70, SD_{W3} = 1.67; F(1,1609) = 27.42, p < .001). It increased more among respondents who have the app.

Intention to follow app's advice is negatively related to the feelings this advice evokes. Moreover, age is positively related to this intention and women show more intention to follow the app's advice (controlling for having the app installed on one's device and past intention to follow the advice). These variables explain 29% of variance in intention to follow the notification.

Table 1. Predictors of intention to follow app's advice

	β	SE	t	p
Intention at wave 2	.31	.02	13.77	<.001
Negative emotional reaction	-.25	.02	-11.54	<.001
Age	.01	.02	4.46	<.001
Gender	.22	.07	3.12	.002
Level of education	.01	.02	0.38	.71
Installation of the app	.48	.08	6.40	<.001

F(6, 1603) =111.8, p < .001, R^2 = .29
Significant predictors are marked in bold

At wave 3, also intention to get tested after the notification was measured. I was on average above the midpoint of the scale (M=4.63, SD=2.16).

9.4.6 Further insights: benefits and concerns related to contact tracing technology

In the first wave of the survey, we measured long- and short-terms concerns related to the introduction of the app. The results showed that these concerns were important for one's motivation to install such an app in the future. Therefore, benefits, concerns and costs related to the app were one of the topics further explored in the survey.

Next to scales used, at wave 1, respondents were asked to freely list their thoughts on potential benefits, concerns and costs of such technology. These thoughts were subsequently coded by trained coders according to a codebook constructed based on past literature on benefits and costs related to new technologies. Based on these codings, items were constructed and included in the third wave of the survey.

An exploratory factor analysis of these items shows five different types of concerns:

1. long-term social concerns (about power of the government and tech companies, *M* = 3.84, *SD* = 1.86, Crobach's alpha = .92),
2. social concerns about others (*M* = 3.17, *SD* = 1.7, Cronbach's alpha = .88),
3. individual concerns (about mobile phone, quarantain and uninstalling the app, *M* = 2.61, *SD* = 1.36, Cronbach's alpha = .63),
4. single-item measuring concerns about misuse of the app (*M* = 3.97, *SD* = 1.99)
5. single-item measuring concerns about access to the app (*M* = 3.53, *SD* = 1.91)

as well as three different types of benefits:

1. Societal health benefits (*M* = 4.52, *SD* = 1.76, Cronbach's alpha = .97)
2. Individual benefits (*M* = 4.44, *SD* = 1.66, Cronbach's alpha = .82),
3. Societal benefits (about impact of using the app on other measures, *M* = 3.24, *SD* = 1.60, Cronbach's alpha = .76).

and two types of costs:

1. costs related to work (*M* = 4.03, *SD* = 2.57, Cronbach's alpha = .89),
2. single-item measuring social costs (*M* = 4.25, *SD* = 2.31)

Looking at the relation of perceived benefits, concerns and costs with installation (controlling for behavior at wave 2, acceptable model fit, pseudo R^2 = .49), societal health benefits have the strongest relation with installation behavior: the more an individual sees the benefits of the app for health on the societal level, the higher the odds of installing the app. At the same time, privacy concerns have the strongest negative relation with installation behavior. Next, social concerns about others impact the behavior negatively. Perceived societal benefits regarding other measures decrease the odds to install the app (possibly as the effectiveness of the app in this regard has not been proven in practice). Finally, individual benefits have the weakest positive relation with behavior, while individual concerns the weakest negative relation. Concerns about fraud, concerns about long-term social consequences and concerns about access to the app do not matter for installation behavior. Looking at demographics, level of education is positively associated with installation behavior.

Table 2. Predictors of installation behavior

	Log(OR)	SE	z	p
Installation at wave 2	3.68	.33	11.07	<.001
Societal health benefits	.73	.08	8.80	<.001
Individual benefits	.17	.08	2.31	.021
Societal benefits	-.19	.07	-2.59	.010
Long-term social concerns	.11	.09	1.18	.237
Social concerns about others	-.31	.09	-3.51	<.001
Individual concerns	-.15	.09	-1.74	.081
Concerns about misuse	.10	.07	1.59	.112
Concerns about lack of access	.06	.05	1.17	.241
Privacy concerns	-.42	.09	-4.70	<.001
Work-related costs	-.05	.03	-1.54	.124
Individual social costs	.10	.04	2.65	.007
Age	.01	.01	1.24	.215
Gender	.15	.16	0.95	.343
Level of education	.12	.05	2.11	.035

χ2 (15) = 1018.25, *p* < .001, *pseudo* R^2 = .49
Significant predictors are marked in bold

9.4.7 Further insights: impact of voluntariness and moral factors

Three factors were measured related to perceived voluntariness of use of contact tracing technology:

- voluntariness from the employer (*M*=6.89, *SD*=1.23, Cronbach's alpha = .9),
- general voluntariness (*M*=6.36, *SD*=1.17, Cronbach's alpha = .65),
- single-item measuring voluntariness in social life (*M*=6.36, *SD*=1.4.

Looking at the impact of voluntariness on app installation, general voluntariness positively relates to the behavior. The other types of voluntariness do not have a significant impact.

Table 3. Predictors of installation behavior

	Log(OR)	SE	z	p
Installation at wave 2	4.06	.29	13.88	<.001
Voluntariness from employer	-.02	.06	-0.41	.686
General voluntariness	.14	.06	2.28	.023
Voluntariness in social life	-.08	.05	-1.58	.115
Age	.02	.004	4.52	<.001
Gender	.02	.13	0.17	.863
Level of education	.18	.04	4.12	<.001

χ2 (7) = 550.81, *p* < .001
Significant predictors are marked in bold

Looking at perceived voluntariness due to one's employment situation, first, respondents' employment status was investigated.

- 53% of respondents are currently working.
- 89% of working respondents are employed (not self-employed).
- 16% of working respondents flexwork.
- 8% of employed respondents flexwork.
- 38% of flex-working respondents do not have a choice.

Installation rates do not differ depending on one's employment contract (among people who are employed). However, having flexible employment interacts with general perceived voluntariness. Namely, for employees with flexible work situation (flex contract or ZZP'er), the more they feel that installation of the app is generally voluntary, the more likely they are to install the app. For employees with non-flexible contract, the perception of voluntariness does not matter.

Table 4. Predictors of installation behavior

	Log(OR)	SE	z	p
Installation at wave 2	4.67	.50	9.40	<.001
Voluntariness from employer	-0.12	.11	-1.18	.237
General voluntariness	0.08	.09	0.87	.384
Voluntariness in social life	0.05	.09	0.50	.621
Flexworking	-2.74	2.57	-1.06	287
Flexworking * voluntariness from employer	-0.24	0.26	-0.95	.341
Flexworking * general voluntariness	0.64	0.32	1.10	.045
Flexworking * voluntariness in social life	-0.02	0.27	-0.08	.935
Age	.02	.01	3.18	<.001
Gender	.02	.18	1.44	.863
Level of education	.18	.07	2.91	<.001

χ2 (10) = 550.81, *p* < .001
Significant predictors are marked in bold

Looking at impact of moral and normative obligations on installing the app, perceived moral obligations strongly increase the odds that one will install the app. Normative obligations do not have a relation with the dependent variable.

Table 5. Predictors of installation behavior

	Log(OR)	SE	z	p
Installation at wave 2	3.91	.34	11.47	<.001
Normative obligations	0.10	.07	1.44	.149
Moral obligations	0.87	.05	17.59	<.001
Age	.01	.01	2.08	.037
Gender	-.001	.17	-0.01	.994
Level of education	.12	.06	2.02	.043

χ2 (6) = 1102.27, *p* < .001
Significant predictors are marked in bold

9.4.8 References

Allen, A. L. (2013). An ethical duty to protect one's own information privacy? *Faculty Scholarship at Penn Law*. 451. Retrieved from: https://scholarship.law.upenn.edu/faculty_scholarship/451

Baek, T. H., & Morimoto, M. (2012). Stay away from me. *Journal of advertising, 41*(1), 59-76.

Bullock, J., Luccioni, A., Hoffmann Pham, K., Sin Nga Lam, C., & Luengo-Oroz, M. (2020). *Mapping the landscape of Artificial Intelligence applications against COVID-19*. https://arxiv.org/pdf/2003.11336.pdf

Dienlin, T., & Metzger, M. J. (2016). An extended privacy calculus model for SNSs: Analyzing self-disclosure and self-withdrawal in a representative US sample. *Journal of Computer-Mediated Communication, 21*(5), 368-383.

Kaushik, A. K., & Rahman, Z. (2015). An alternative model of self-service retail technology adoption. *Journal of Services Marketing.*

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research, 15*(4), 336-355.

Posch, K., Jackson, J., Bradford, B., & Macqueen, S. (2020). "Truly free consent"? Clarifying the nature of police legitimacy using causal mediation analysis*. Journal of Experimental Criminology,* 1-33.

Watson, D., Clark, L. A., & Tellegen, A. (1988). Development and validation of brief measures of positive and negative affect: the PANAS scales*. Journal of personality and social psychology, 54*(6), 1063.

Appendix 1 Advisory board

- Prof. Dr. Barbara Baarsma *Professor of Applied Economics* at University of Amsterdam
- Prof. Dr. Moniek Buijzen *Professor of Communication and Behavioral Change* at Erasmus University Rotterdam
- Prof. Dr. Niels Chavannes *Professor of Primary Care Medicine* at Leiden University Medical Center
- Dr. Virginia Dignum *Associate Professor at the Faculty of Technology Policy and Management* at Delft University of Technology
- Prof. Dr. José van Dijck *University Professor Media and Digital Society* at Utrecht University
- Prof. Dr. Huub Dijstelbloem *Professor of Philosophy of Science and Politics* at University of Amsterdam
- Prof. Dr. Valerie Frissen *Professor Digital Technologies and Social Change* at Leiden University
- Dr. Seda Gürses *Associate Professor in the Department of Multi-Actor Systems* at Delft University of Technology
- Prof. Dr. Albert Meijer *Professor of Public Innovation* at Utrecht University
- Prof. Dr. Beate Roessler *Professor of Ethics* at University of Amsterdam
- Marietje Schaake *International Policy Director* at Stanford University
- Dr. Mirko Schaefer *Associate Professor Humanities* at Utrecht University
- Prof. Dr. Ir. Maarten van Steen *Scientific Director Digital Society Institute* at University of Twente
- Dr. Linnet Taylor *Associate Professor at the Tilburg Institute for Law, Technology, and Society* at Tilburg University
- Dr. Michael Veale *Lecturer Digital Rights and Regulation* at University College London
- Prof. Dr. Sally Wyatt *Professor of Digital Cultures* at Maastricht University

Appendix 2 List of contributions to the media, public and academic discourse

Publications

- Eskens, S. and Helberger, N., Regulating Digital Contact Tracing for Communicable Diseases (to be submitted to an international journal)

- Helberger, N. Eskens, S. Toh, J. Bouché, G. and Appelman, N., Big tech platforms as 'societal problem solvers': How to organise democratic oversight and control (to be submitted to an international journal)

- Mill, J., Appeldoorn, J., Van Hoboken, J. and Eskens, S., Regulating the use of mobility data for health (to be submitted to a Dutch or international journal)

Commissioned expert opinions

- Sharon, T., The Googlization of Pandemic Response: Ethical Concerns Regarding Digital Contact Tracing and Big Tech

- Schaeffer, M., Considering Ethical issues of invasive technologies. Data Ethics Decision Aid (DEDA) & CoronaMelder

- Poort, J., CoronaMelder: An Economic Perspective

Newspaper op-ed

- **Corona App vraagt om meer toezicht op grote techbedrijven**
  https://www.volkskrant.nl/columns-opinie/opinie-corona-app-vraagt-om-meer-toezicht-op-grote-techbedrijven~b6898138/

  Outlet: De Volkskrant
  Author(s): Natali Helberger, Sarah Eskens
  September 10, 2020

- **Doorsturen telecomdata naar RICM vereist een beter verhaal**
  https://fd.nl/opinie/1356879/doorsturen-telecomdata-naar-rivm-vereist-een-beter-verhaal

  Outlet: Het Financieel Dagblad
  Author(s): Sarah Eskens, Jurriaan van Mil
  Date: September 11, 2020

-

- **Beleid voor Coronacheck ontbreekt jammerlijk**
  https://www.nrc.nl/nieuws/2021/04/25/beleid-voor-coronacheck-apps-ontbreekt-jammerlijk-a4041219

  Outlet: NRC
  Author(s): Natali Helberger, Marijn Sax, Joanna Strycharz
  Date: April 25, 2021

Media coverage Newspaper

- **Filosofen over de Corona app: Begrijpt de overheid privacy wel?**
  https://www.trouw.nl/nieuws/filosofen-over-de-corona-app-begrijpt-de-overheid-privacy-wel~be38a475/

  Outlet: Trouw
  Expert(s): Marijn Sax
  Date: April 10, 2020

- **Testlijnmedewerkers kunnen bij persoonsgegevens, ook als dat niet mag**
  Testlijnmedewerkers kunnen bij persoonsgegevens, ook als dat niet mag | Nieuwsuur (nos.nl)

  Outlet: Nieuwsuur NOS
  Expert(s): Sarah Eskens
  Date: September 16, 2020

- **Door alle technische problemen wegen voordelen CoronaMelder niet op tegen nadelen**
  'Door alle technische problemen wegen voordelen CoronaMelder niet op tegen nadelen' - Folia

  Outlet: FOLIA
  Expert(s): Joran van Apeldoorn
  Date: October 29, 2020

- **Het geloof in de testsamenleving vertoont scheurtjes: het kan matschappelijke tegenstellingen versterken.**
  https://www.nrc.nl/nieuws/2021/04/23/het-geloof-in-de-testsamenleving-vertoont-scheurtjes-het-kan-maatschappelijke-tegenstellingen-versterken-a4041082

  Outlet: NRC
  Expert(s): Marijn Sax
  Date: April 23, 2021

Media coverage Television

- **Nieuwsuur**
  Expertbijdrage over AVG schending door callcenters van de GGD tijdens de coronacrisis
  https://www.npostart.nl/nieuwsuur/16-09-2020/VPWON_1310915

  Outlet: Nieuwsuur, NOS
  Date: September 16, 2020
  Expert(s): Sarah Eskens

Media coverage Radio

- **De CoronaMelder-app heeft meer nadelen dan voordelen**
  De CoronaMelder-app heeft meer nadelen dan voordelen | NPO Radio 1

  Outlet: NPO Radio 1
  Date: November 2, 2020
  Expert(s): Joran van Apeldoorn

Presentations

- **iBestuur Congres 2020**
  https://ibestuurcongres.nl/
  Sessie 'Ethiek en digitalisering' – Reflectie op de nationale discussie over de corona-app en de inzet van telecomdata

  Place: online
  Date: September 11, 2020
  Speaker(s): Natali Helberger

- **Wemakethe.city 2020: RESET: Healthcare**
  https://dezwijger.nl/programma/reset-healthcare
  Panel discussion at Pakhuis de Zwijger

  Place: Amsterdam, the Netherlands
  Date: September 21, 2020
  Speaker(s): Sarah Eskens

- **Werkbezoek Minister van Engelshoven at University of Amsterdam**
  Presentation: AI toepassingen in de COVID-19 pandemie

  Date: September 27, 2020
  Speaker(s): Joanna Strycharz

- **TechTalk #2 at de Rode Hoed: Privacy en de CoronaMelder**
  https://rodehoed.nl/stream/techtalks-2-corona-app/

  Place: Amsterdam, the Netherlands
  Date: December 8, 2020
  Speaker(s): Sarah Eskens

- **Guest lecture Advanced Master's students in Law and Digital Technologies at Leiden Law School, Leiden University**
  Online lecture on "Legal, Ethical and Societal Implications of Contact Tracing Apps"

  Date: December 10, 2020
  Speaker(s): Natali Helberger

Conferences

- **Digital data and emerging technologies: Problems and perspectives for the law**
  Digital technologies for corona: Moving beyond the rights to privacy and data protection.

  Place: online conference, Italy
  Date: March 9, 2021
  Speaker(s): Sarah Eskens

- **TILTing Perspectives 2021: Regulating in times of crisis**
  Panel: Big Tech Platforms as 'societal problem solvers':
  How to organise democratic oversight and control.
  https://easychair.org/smart-program/TILTing2021/

  Place: Tilburg, Netherlands
  Date: May 20, 2021
  Speaker(s): Sarah Eskens, Natali Helberger, Jill Toh, Gionata Bouchè and Naomi Appelman.

- **TILTing Perspectives 2021: Regulating in times of crisis**
  Panel: Digital technologies during COVID-19: A multi-disciplinary problematization of privacy's value hegemony.
  https://easychair.org/smart-program/TILTing2021/

  Place: Tilburg, Netherlands
  Date: May 20, 2021
  Speaker(s): Sarah Eskens, Tamar Sharon, Marjolein Lanzing, Lotje Siffels, Natali Helberger, Joanna Strycharz, Joran van Apeldoorn and Marijn Sax.

- **Privacy Law Scholars Conference 2021 (PLSC)**
  Regulating Digital Contact Tracing for Communicable Diseases
  https://privacyscholars.org/

  Date: June 3, 2021
  Speaker(s): Natali Helberger, Sarah Eskens

- **Human rights in times of pandemic: political exceptionalism, social vulnerabilities & confined liberties: international and European perspectives**

  Date: 6-7 September, 2021
  Speaker(s): Sarah Eskens

Appendix 3
Codebooks

Survey Wave 1: Codebook

INFORMATIEBROCHURE VOOR DEELNEMERS AAN ONDERZOEK
“Technologie en samenleving”

Beste deelnemer,

Dit onderzoek voeren we uit in opdracht van de Universiteit van Amsterdam (UvA).

Voordat u aan het onderzoek begint, wil de UvA u een aantal zaken laten weten. Het is belangrijk dat u op de hoogte bent van de procedure die in dit onderzoek wordt gevolgd. Lees daarom onderstaande tekst alstublieft zorgvuldig door en aarzel niet om opheldering te vragen over de tekst. De UvA-onderzoekers beantwoorden eventuele vragen graag.

Doel van het onderzoek

In deze vragenlijst wordt naar uw mening over technologie en de samenleving gevraagd. Het doel van dit onderzoek is om het gedrag en de opvattingen van Nederlanders ten opzichte van dit onderwerp beter te begrijpen. We zullen u in de toekomst nog driemaal uitnodigen voor een korte vragenlijst over technologie en de samenleving.

Gang van zaken tijdens het onderzoek

Als u akkoord gaat met deelname aan dit onderzoek, zal u een aantal vragen over technologie en de samenleving krijgen. Daarnaast wordt er gevraagd naar uw mening over de gebeurtenissen rondom de coronacrisis en naar uw media consumptie (bijvoorbeeld of u kranten leest). We vragen u ook naar uw geboorteland en het geboorteland van uw ouders omdat we uit onderzoek weten dat er meer mensen door het coronavirus overlijden onder etnische minderheden. Wij willen onderzoeken of minderheden ook meer kwetsbaar zijn voor of anders aankijken tegen de risico’s van digitale technologieën. U kunt ervoor kiezen om deze vragen niet te beantwoorden. De vragenlijst duurt ongeveer 20 minuten.

Vertrouwelijkheid van gegevens

Uw persoonsgegevens (persoonlijke informatie) blijven vertrouwelijk en worden niet gedeeld met anderen zonder uw uitdrukkelijke toestemming. De onderzoeksgegevens worden voor wetenschappelijk onderzoek geanalyseerd door de onderzoekers van dit project. De onderzoeksresultaten worden gebruikt in wetenschappelijke publicaties. De data zullen daarvoor openbaar worden gemaakt, maar dit zal volledig geanonimiseerd gebeuren.

Vrijwilligheid

U kunt uw medewerking ten alle tijden staken zonder opgave van redenen. Tevens kunt u zeven dagen na dit onderzoek alsnog uw toestemming intrekken. Mocht u uw medewerking nu staken of achteraf uw toestemming intrekken, dan zullen uw gegevens worden verwijderd uit onze bestanden en vernietigd.

TOESTEMMINGSVERKLARING

Als u akkoord gaat, verklaart u dat u de deelnemersinformatie heeft gelezen en begrepen. Verder geeft u met de ondertekening te kennen dat u akkoord gaat met de gang van zaken zoals deze staat beschreven op de vorige pagina.

Als u nog verdere informatie over het onderzoek zou willen krijgen kunt u zich wenden tot de verantwoordelijke onderzoeker, Dr. Joanna Strycharz, email j.strycharz@uva.nl, Nieuwe Achtergracht 166, 1001 NG Amsterdam.

Mochten er naar aanleiding van uw deelname aan dit onderzoek bij u klachten of opmerkingen zijn, dan kunt u contact opnemen met het lid van de Commissie Ethiek namens de Amsterdam School of Communication Research, per adres:

ASCoR Secretariat,
Ethics Committee,
University of Amsterdam,
PO Box 15793,
1001 NG Amsterdam;
020-525 3680;
ascor-secr-fmg@uva.nl.

Een vertrouwelijke behandeling van uw klacht of opmerking is daarbij gewaarborgd.

[DEELNEMER]

- *Ik ben 16 jaar of ouder.*
- *Ik heb de informatie gelezen en begrepen.*
- *Ik stem toe met deelname aan het onderzoek en gebruik van de daarmee verkregen gegevens.*
- *Ik behoud het recht om zonder opgaaf van reden deze instemming weer in te trekken binnen 7 dagen na afloop van dit onderzoek.*
- *Als mijn onderzoeksresultaten gebruikt worden in wetenschappelijke publicaties, of op een andere manier openbaar worden gemaakt, dan zal dit volledig geanonimiseerd gebeuren. Mijn persoonsgegevens worden niet door derden ingezien zonder mijn uitdrukkelijke toestemming.*

- *Ik behoud het recht op ieder door mij gewenst moment te stoppen met het onderzoek.*

[CONS]
1 = akoord / 2 = niet akkoord

BLOCK: TECHNOLOGY USE AND ADOPTION

Q1 [TECH_OPEN]
Tijdens de coronacrisis worden digitale technologieën ingezet om de verspreiding van de ziekte tegen te gaan.

Van welke digitale technologieën heeft u gehoord?

Open

Intro
Wij willen graag uw mening weten over specifieke digitale technologieën die worden ingezet om de verspreiding van corona tegen te gaan.

Q2.1 [APP_AWE]
De overheid werkt op dit moment aan een app die u waarschuwt als u in de buurt bent geweest van iemand die later positief is getest op het coronavirus.

Was u op de hoogte van deze app voordat u deelnam aan deze studie?

1 = Ja 2 = Nee

Q2.2 [APP_WORK]
Hoe stelt u zich de werking van een dergelijke app voor?

Open

[APP_INTRO]
Een contact-tracing app herkent via Bluetooth andere telefoons in de buurt die de app ook gebruiken (Bluetooth is een methode om draadloos gegevens uit te wisselen tussen twee of meer apparaten. Dat gebeurt met radiogolven). Als u langere tijd dicht bij een andere gebruiker bent, slaat uw app de anonieme code van de andere gebruiker op. Een gebruiker die positief is getest voor het coronavirus kan dit vrijwillig in de app melden. De app van deze gebruiker stuurt de eigen anonieme codes van de afgelopen dagen naar een centrale server. De app ziet geen persoonsgegevens en legt niet vast waar u bent. Deze app stuurt u een bericht als u enige tijd dicht bij iemand in de buurt bent geweest die besmet is met het coronavirus.

Q2.3 [APP_BEN]
Wat zijn volgens u de voordelen van het gebruik van een contact-tracing app?

Open

Q2.4 [APP_COST]
Wat zijn volgens u de nadelen van het gebruik van een contact-tracing app?

Open

Q 3 [MOTIV]
In hoeverre bent u gemotiveerd om:

MOTIV1 De eerdergenoemde contact-tracing app op uw mobiele telefoon te installeren.
MOTIV2 Persoonlijke gegevens van uw mobiele telefoon te delen bij een verplichte quarantaine (bijv. als u de ziekte heeft of uit bepaalde landen terugkomt) zodat de overheid kan controleren of u zich aan de quarantaine houdt.
MOTIV3 Uw lichaamstemperatuur te laten meten in winkels en restaurants om te controleren of uw mogelijk ziek bent.
MOTIV4 Een mobiele app installeren die laat zien dat u gezond bent als u winkels, restaurants en publieke evenementen wilt bezoeken.
MOTIV 5 Een app te gebruiken om corona-gerelateerde klachten te laten beoordelen door medische specialisten.
1. Helemaal niet gemotiveerd - 7. Helemaal wel gemotiveerd

Q 4 [APP_MOTIV]
Stelt u zich voor dat de overheid de bovengenoemde contact-tracing app beschikbaar maakt. In hoeverre zou u uw gegevens willen delen via de contact-tracing app?

APP_MOTIV1 In hoeverre bent u bereid om uw gegevens te delen via de contact-tracing app?

1. Zeer onbereid - 7. Zeer bereid

APP_MOTIV2 Hoe aannemelijk is het dat u uw gegevens zou delen via de contact-tracing app?

1 Zeer onaannemelijk - 7 Zeer aannemelijk

BLOCK: INDIVIDUELE KENMERKEN

Q 5 [INFO_SOURCE]
Hoeveel keer per week heeft u in de afgelopen maand van de volgende bronnen informatie over het coronavirus ontvangen?

INFO_SOURCE1 Nieuws op televisie (bijv. NOS Journaal, RTL Nieuws)
INFO_SOURCE2 Actualiteitenprogramma's op televisie (bijv. EenVandaag, Nieuwsuur)
INFO_SOURCE3 Talkshows op televisie (bijv. Jinek, Op1, Beau)
INFO_SOURCE4 Papieren of digitale kranten, maar niet de website (bijv. De Telegraaf, Algemeen Dagblad, De Volkskrant)
INFO_SOURCE5 Papieren of digitale tijdschriften (bijv. LINDA, Kampioen, Elsevier)

INFO_SOURCE6 Radionieuws (bijv. NPO Radio 1, SkyRadio)
INFO_SOURCE7 Websites van televisienieuws (bijv. nos.nl, rtlnieuws.nl)
INFO_SOURCE8 Websites van kranten (bijv. telegraaf.nl, ad.nl, nrc.nl, volkskrant.nl)
INFO_SOURCE9 Andere nieuwswebsites (exclusief sociale media, bijv. nu.nl, geenstijl.nl)
INFO_SOURCE10 Gezondheidswebsites (bijv. thuisarts.nl, gezondheidsplein.nl)
INFO_SOURCE11 Overheidswebsites (bijv. rivm.nl, rijksoverheid.nl)
INFO_SOURCE12 Nieuwsapps (op uw mobiele telefoon of tablet, bijv. nu.nl app, nos app)
INFO_SOURCE13 Overige apps (bijv. gezondheidsapps)
INFO_SOURCE14 Sociale media (bijv. Facebook, Twitter, YouTube)
INFO_SOURCE15 Chatprogramma's (bijv. WhatsApp, Telegram, WeChat)

0. Nooit
1. 1 dag per week
2. 2 dagen per week
3. 3 dagen per week
4. 4 dagen per week
5. 5 dagen per week
6. 6 dagen per week
7. 7 dagen per week

Routing – Als iemand >1 kiest bij items van Q5 à bijhorende items van Q6

Q6 [INFO_TRUST]
De volgende vraag gaat over **de informatie die u consumeert** over het **coronavirus.** Geef hieronder aan in welke mate u de volgende bronnen vertrouwt:

INFO_TRUST1 Nieuws op televisie (bijv. NOS Journaal, RTL Nieuws)
INFO_TRUST2 Actualiteitenprogramma's op televisie (bijv. EenVandaag, Nieuwsuur)
INFO_TRUST3 Talkshows op televisie (bijv. Jinek, Op1, Beau)
INFO_TRUST4 De papieren of digitale editie, maar niet de website (bijv. De Telegraaf, Algemeen Dagblad, De Volkskrant)
INFO_TRUST5 De papieren of digitale editie (bijv. LINDA, Kampioen, Elsevier)
INFO_TRUST6 Zowel offline als online (bijv. NPO Radio 1, SkyRadio)
INFO_TRUST7 Websites van televisienieuws (bijv. nos.nl, rtlnieuws.nl)
INFO_TRUST8 Websites van kranten (bijv. telegraaf.nl, ad.nl, nrc.nl, volkskrant.nl)
INFO_TRUST9 Andere nieuwswebsites (exclusief sociale media, bijv. nu.nl, geenstijl.nl)
INFO_TRUST10 Gezondheidswebsites (bijv. thuisarts.nl, gezondheidsplein.nl)
INFO_TRUST11 Overheidswebsites (bijv. rivm.nl, rijksoverheid.nl)
INFO_TRUST12 Nieuwsapps (op uw mobiele telefoon of tablet, bijv. nu.nl app, nos app)
INFO_TRUST13 Overige apps (bijv. gezondheidsapps)
INFO_TRUST14 Sociale media (bijv. Facebook, Twitter, YouTube)
INFO_TRUST15 Chatprogramma's (bijv. WhatsApp, Telegram, WeChat)

1. Vertrouw ik helemaal niet als informatiebron. - 7. Vertrouw ik heel erg als informatiebron

Q7 [EVENTS]
In hoeverre heeft u gehoord van de volgende gebeurtenissen rondom de coronacrisis?

EVENTS1 Half juni werd er een lokale lockdown in Duitsland ingesteld vanwege een corona-uitbraak in de vleesindustrie.
EVENTS2 Op 22 juni waren er voor het eerst sinds de start van de crisis in Nederland geen nieuwe sterfgevallen.
EVENTS3 Er was een demonstratie in Den Haag tegen de coronamaatregelen.
EVENTS4 De RIVM-infectieradar website had een datalek.
EVENTS5 De regering heeft een voorstel ingediend voor een coronawet, (Tijdelijke Wet Maatregelen Covid-19), die in plaats van de noodverordening moest komen.
EVENTS6 Het RIVM heeft toestemming gekregen om zendmastdata te verwerken in de strijd tegen corona.
EVENTS7 Het Ministerie van Volksgezondheid, Welzijn en Sport organiseerde een "Appathon" om een contact-tracing app te ontwikkelen

1. Niets van gehoord. 2. Iets van gehoord. 3. Veel over gehoord

Q 8 [HEALTH_STAT]
HEALTH_STAT1 Hoe zou u uw gezondheid omschrijven?
1. Slecht - 7. Uitstekend – 8. Zeg ik liever niet

HEALTH_STAT2 Hoe bezorgd bent u over uw gezondheid?

1. Helemaal niet bezorgd - 7. Heel erg bezorgd 8 Zeg ik liever niet

HEALTH_STAT3 Ik ben vaker ziek dan andere mensen van dezelfde leeftijd en hetzelfde geslacht.

1. Helemaal mee oneens - 7. Helemaal mee eens 8 Zeg ik liever niet

Q10 [ACCEPT]
In hoeverre vindt u de onderstaande manieren acceptabel om de verspreiding van de ziekte tegen te houden?

ACCEPT1 Geautomatiseerd berichten op sociale media analyseren om het verspreiden van foute informatie over het virus te voorkomen.
ACCEPT2 Het gebruik van apps om bij te houden wanneer je in de buurt bent geweest van iemand die besmet is.
ACCEPT3 Het gebruik van locatiegegevens van mobiele telefoons om mensen te volgen die mogelijk besmettelijk zijn.
ACCEPT4 Het gebruik van gezichtsherkenning om mensen te volgen die mogelijk besmettelijk zijn.
ACCEPT5 Het monitoren van smartphone gebruik om na te gaan of mensen zich aan de verplichte quarantaine te houden.
ACCEPT6 Het inzetten van kunstmatige intelligentie om een medicijn tegen het coronavirus te vinden.
ACCEPT7 Het inzetten van digitale communicatiediensten zoals Whatsapp door de overheid om snel informatie te delen met de bevolking.

ACCEPT8 Het gebruik van apps om mensen zelf hun corona-gerelateerde klachten te laten beoordelen.
ACCEPT9 Het invoeren van een immuniteitspaspoort (dit is een officiële verklaring dat deze persoon covid-19 doorgemaakt heeft gehad en is immuun is).
ACCEPT10 Het gebruik van drones om mensen te waarschuwen.
ACCEPT11 De inzet van robots in restaurants, verpleeghuizen of overheidsinstellingen om menselijk contact te verminderen.
ACCEPT12 Het testen van rioolwater op aanwezigheid van coronavirus.

1. Helemaal niet acceptabel - 7. Helemaal wel acceptabel
9. Weet ik niet

____

Q11 [PRIV_CON]
Er volgt nu een aantal specifieke stellingen over gebruik van de contact-tracing app. Geef voor iedere stelling aan of u het hiermee oneens of eens bent.

PRIV_CON1 Ik ben bezorgd dat gegevens verzameld via de app misbruikt kunnen worden door anderen wanneer ik de contact-tracing app gebruik.
PRIV_CON2 Wanneer ik de contact-tracing app gebruik heb ik het gevoel dat anderen mijn locatie kunnen bijhouden.
PRIV_CON3 Ik ben bang dat mijn gegevens verzameld via de contact-tracing app die ik deel via de contact-tracing app niet veilig worden opgeslagen.
PRIV_CON4 Ik ben bezorgd dat gegevens verzameld via de contact-tracing app verder worden verspreid naar andere partijen.
PRIV_CON5 Ik ben bezorgd dat gegevens verzameld via de contact-tracing app gezien of gehoord worden door mensen die ik niet ken.
PRIV_CON6 Ik ben bang dat gegevens verzameld via de contact-tracing app voor andere doeleinden worden gebruikt.
PRIV_CON7 Ik ben bezorgd dat ik geen controle heb over wie mijn gegevens verzameld via de contact-tracing app kan inzien.

1. Helemaal mee oneens - 7. Helemaal mee eens

____

Q12 [CONS_OTHER]
In hoeverre bent u het eens of niet eens met de volgende stellingen?

CONS_OTHER1 Ik maak me zorgen dat het gebruik van de app negatieve gevolgen zal hebben voor kwetsbare groepen in de maatschappij.
CONS_OTHER2 Ik ben bezorgd dat het gebruik van de app ertoe kan leiden dat mensen ongelijk behandeld worden.
CONS_OTHER3 Ik ben bang dat als ik de contact-tracing app installeer, ik hem niet meer kan verwijderen.
CONS_OTHER4 Ik maak me zorgen dat als ik de contact-tracing app installeer, ik door de app gevolgd wordt.
CONS_OTHER5 Ik ben bang dat als ik de contact-tracing app **niet** installeer, ik geen toegang meer heb tot de publieke ruimte.

1. Helemaal mee oneens - 7. Helemaal mee eens

Q13 [NORM]
In hoeverre bent u het eens met de volgende stellingen?

U kunt bij deze stellingen dan een inschatting maken van wat u zou vinden als u gebruik zou maken van de contact-tracing app.

NORM1 Mensen die belangrijk voor mij zijn, vinden dat ik de contact-tracing app moet gebruiken.
NORM2 Mensen die invloed op mij hebben, vinden dat ik de contact-tracing app moet gebruiken.
NORM3 De meeste mensen die ik ken zouden de contact-tracing app installeren.
NORM4 Er wordt van je verwacht dat je de contact-tracing app installeert.

1. Helemaal mee oneens - 7. Helemaal mee eens

Q14 [SUSC] [SEVER]
Deze vragen gaan over uw kans om het coronavirus te krijgen. Ook als u eerder al besmet bent geweest met het coronavirus, vul deze vragen dan alstublieft in.

SUSC1 Hoe groot is de kans dat u de komende maanden besmet raakt met het coronavirus?

1. Erg klein - 7. Erg groot
9. Weet ik niet / wil niet zeggen

SEVER1 Hoe erg zou het voor u zijn, als u het coronavirus krijgt?

1. Helemaal niet erg - 7. Heel erg
9. Weet ik niet / wil niet zeggen

SUSC2 Stel dat u zelf besmet bent met het coronavirus. Hoe waarschijnlijk is het dan dat u weer anderen zal besmetten?

1. Zeer onwaarschijnlijk - 7. Zeer waarschijnlijk
9. Weet ik niet / wil niet zeggen

SEVER2 Hoe erg zou u het vinden om iemand anders te besmetten met het coronavirus?

1. Helemaal niet erg - 7. Heel erg
9. Weet ik niet / wil niet zeggen

Q15 [DIGI_EFF]
Hoeveel vertrouwen heeft u dat u de volgende activiteiten kunt uitvoeren?

DIGI_EFF1 Het vinden van informatie op het internet.
DIGI_EFF2 Online communiceren met anderen.
DIGI_EFF3 Het downloaden en uploaden van bestanden.
DIGI_EFF4 Praten over internet hardware, zoals netwerken of routers.
DIGI_EFF5 Praten over internet software, zoals zoekmachines en webbrowsers.

DIGI_EFF6 Internetproblemen oplossen.
DIGI_EFF7 Het gebruiken van apps op mijn mobiel.
DIGI_EFF8 Hulp vinden om mijn vragen over internet te beantwoorden als ik dat nodig heb.

1. helemaal geen vertrouwen - 7. heel veel vertrouwen

____

Q16 [TRUST_GOV]
In hoeverre bent u het eens of oneens met de volgende stellingen?

TRUST_GOV1 De overheid is betrouwbaar in het behandelen van mijn persoonlijke data
TRUST_GOV2 Ik vertrouw erop dat de overheid goed met mijn persoonlijke data omgaat
TRUST_GOV3 De overheid is eerlijk als het gaat om het gebruik van mijn persoonlijke data

1. Helemaal mee oneens - 7. Helemaal mee eens

____

Q17 [RISK_GOV]
In hoeverre bent u het eens of oneens met de volgende stellingen?

RISK_GOV1 In het algemeen is het riskant om mijn persoonlijke data aan de overheid te geven
RISK_GOV2 Ik verlies mijn privacy als ik mijn persoonlijke data aan de overheid verstrek
RISK_GOV3 Er is te veel onzekerheid bij het geven van mijn persoonlijke data aan de overheid
RISK_GOV4 Persoonlijke gegevens die ik deel kunnen door de overheid voor andere doeleinden worden gebruikt.
RISK_GOV5 Ik voel me veilig om mijn persoonlijke data af te staan aan de overheid

1. Helemaal mee oneens - 7. Helemaal mee eens

____

Q18 [TRUST_TECH]
In hoeverre bent u het oneens of eens met de volgende stellingen?

TRUST_TECH1 Techbedrijven zoals Google of Apple zijn betrouwbaar in het behandelen van mijn persoonlijke data
TRUST_TECH2 Ik vertrouw erop dat techbedrijven zoals Google of Apple mijn persoonlijke data te goeder trouw behandelen
TRUST_TECH3 Techbedrijven zoals Google of Apple zijn eerlijk als het gaat om het gebruik van mijn persoonlijke data.

1. Helemaal mee oneens - 7. Helemaal mee eens

____

Q19 [RISK_TECH]
RISK_TECH1 In het algemeen is het riskant zijn om mijn persoonlijke data aan techbedrijven zoals Google of Apple te geven

RISK_TECH2 Ik verlies mijn privacy als ik mijn persoonlijke data aan techbedrijven zoals Google of Apple verstrekt
RISK_TECH3 Er is te veel onzekerheid bij het geven van mijn persoonlijke data aan techbedrijven zoals Google of Apple
RISK_TECH4 Persoonlijke gegevens die ik deel kunnen voor andere doeleinden worden gebruikt.
RISK_TECH5 Ik voel me veilig om mijn persoonlijke data af te staan aan techbedrijven zoals Google of Apple

1. Helemaal mee oneens - 7. Helemaal mee eens

____

Q20 [BEH_CHANGE]
In hoeverre zijn de volgende stellingen op u van toepassing?

BEH_CHANGE1 Ik haal meer boodschappen in huis dan ik gewoonlijk doe.
BEH_CHANGE2 Ik blijf zoveel mogelijk thuis.
BEH_CHANGE3 Ik help anderen in nood.
BEH_CHANGE4 Ik was vaker en langer mijn handen.
BEH_CHANGE5 Ik ga alleen naar de winkel als het noodzakelijk is
BEH_CHANGE6 Ik werk thuis
BEH_CHANGE7 Ik nies en hoest in mijn elleboog.
BEH_CHANGE8 Ik houd 1.5 meter afstand van andere mensen (social distancing)

1. Helemaal niet - 7. Helemaal wel

____

Q21 [WELL_B]
Als het gaat om de afgelopen 7 dagen, hoe vaak…

WELL_B1 Voelde u zich erg zenuwachtig?
WELL_B2 Zat u zo erg in de put dat niets u kon opvrolijken?
WELL_B3 Voelde u zich kalm en rustig?
WELL_B4 Voelde u zich neerslachtig en somber?
WELL_B5 Voelde u zich gelukkig?

1. Nooit
2. Zelden
3. Soms
4. Vaak
5. Meestal
6. Voortdurend
7. Zeg ik liever niet

BLOCK: KENMERKEN VAN DE APP

Q22 [ACCEPT_DATA]

In hoeverre vindt u het acceptabel als de volgende partijen toegang krijgen tot uw persoonlijke gezondheidsgegevens die via de contact-tracing app verzameld worden?

ACCEPT_DATA1 Vrienden
ACCEPT_DATA2 Familie
ACCEPT_DATA3 De Nederlandse overheid
ACCEPT_DATA4 Een buitenlandse overheid
ACCEPT_DATA5 Het Rijksinstituut voor Volksgezondheid en Milieu (RIVM)
ACCEPT_DATA6 De Gemeentelijke Gezondheidsdienst (GGD)
ACCEPT_DATA7 Huisartsen
ACCEPT_DATA8 Ziekenhuizen
ACCEPT_DATA9 Apothekers
ACCEPT_DATA10 Uw zorgverzekeraar
ACCEPT_DATA11 Andere zorgverzekeraars dan uw zorgverzekeraar
ACCEPT_DATA12 Uw werkgever
ACCEPT_DATA13 Adverteerders
ACCEPT_DATA14 Google
ACCEPT_DATA15 Facebook
ACCEPT_DATA16 Politieke partijen

1. onacceptabel - 7. acceptabel

____

Q24 [ACCEPT_AIM]
Voor welke van onderstaande doelen vindt u het acceptabel als corona-apps uw persoonlijke gegevens verzamelen?

Ik vind het acceptabel als corona-apps mijn persoonlijke gegevens verzamelen met als doel...

ACCEPT_AIM1 mijn gezondheid te verbeteren.
ACCEPT_AIM2 de gezondheidszorg in het algemeen te verbeteren.
ACCEPT_AIM3 de maatschappij te helpen in de strijd tegen coronavirus
ACCEPT_AIM4 wetenschappelijk onderzoek te doen.
ACCEPT_AIM5 deze gegevens te verstrekken aan het Rijksinstituut voor Volksgezondheid en Milieu (RIVM).
ACCEPT_AIM6 deze gegevens te verstrekken aan de Gemeentelijke Gezondheidsdienst (GGD).
ACCEPT_AIM7 deze gegevens te verstrekken aan mijn zorgaanbieder, zoals mijn huisarts.
ACCEPT_AIM8 deze gegevens te verstrekken aan zorgverzekeraars.
ACCEPT_AIM9 deze gegevens te verstrekken aan mijn werkgever.

1. helemaal mee oneens - 7. helemaal mee eens

DEMOGRAFISCHE GEGEVENS

De volgende vragen gaan over het geboorteland van u en uw ouders. Deze worden gebruikt om uw land van herkomst te bepalen. U bent niet verplicht te antwoorden. Door te antwoorden geeft u uitdrukkelijk toestemming aan ons om deze gegevens alleen voor onderzoeksdoeleinden te gebruiken. De gegevens worden volstrekt vertrouwelijk behandeld en niet aan derden verstrekt.

In welk land bent u zelf en in welk land zijn uw ouders geboren?

Q25 [GEB] Zelf: _______________
Q26 [GEB_V] Vader: _______________
Q27 [GEB_M] Moeder: _______________

- Nederland
- Turkije
- Marokko
- Suriname
- Nederlandse Antillen / Aruba
- Bulgarije
- Polen
- Roemenië
- Indonesië / voormalig Nederlands-Indië
- Japan
- Verenigde Staten, Canada
- Australië, Nieuw-Zeeland
- Ander Europees land
- Ander niet-Europees land
- Weet ik niet
- Wil ik niet zeggen

Survey Wave 2: Codebook

INFORMATIEBROCHURE VOOR DEELNEMERS AAN ONDERZOEK

"Technologie en samenleving"

Beste deelnemer,

Dit onderzoek voeren we uit in opdracht van de Universiteit van Amsterdam (UvA). Voordat u aan het onderzoek begint, wil de UvA u een aantal zaken laten weten. Het is belangrijk dat u op de hoogte bent van de procedure die in dit onderzoek wordt gevolgd. Lees daarom onderstaande tekst alstublieft zorgvuldig door en aarzel niet om opheldering te vragen over de tekst. De UvA-onderzoekers beantwoorden eventuele vragen graag.

Doel van het onderzoek

In deze vragenlijst wordt naar uw mening over technologie en de samenleving gevraagd. Het doel van dit onderzoek is om het gedrag en de opvattingen van Nederlanders ten opzichte van dit onderwerp beter te begrijpen. We zullen u in de toekomst nog driemaal uitnodigen voor een korte vragenlijst over technologie en de samenleving.

Gang van zaken tijdens het onderzoek

Als u akkoord gaat met deelname aan dit onderzoek, zal u een aantal vragen over technologie en de samenleving krijgen in de huidige coronacrisis. De vragenlijst duurt ongeveer 15 minuten.

Vertrouwelijkheid van gegevens

Uw persoonsgegevens (persoonlijke informatie) blijven vertrouwelijk en worden niet gedeeld met anderen zonder uw uitdrukkelijke toestemming. De onderzoeksgegevens worden voor wetenschappelijk onderzoek geanalyseerd door de onderzoekers van dit project. De onderzoeksresultaten worden gebruikt in wetenschappelijke publicaties. De data zullen daarvoor openbaar worden gemaakt, maar dit zal volledig geanonimiseerd gebeuren.

Vrijwilligheid

U kunt uw medewerking ten alle tijden staken zonder opgave van redenen. Tevens kunt u zeven dagen na dit onderzoek alsnog uw toestemming intrekken. Mocht u uw medewerking nu staken of achteraf uw toestemming intrekken, dan zullen uw gegevens worden verwijderd uit onze bestanden en vernietigd.

TOESTEMMINGSVERKLARING

Als u akkoord gaat, verklaart u dat u de deelnemersinformatie heeft gelezen en begrepen. Verder geeft u met de ondertekening te kennen dat u akkoord gaat met de gang van zaken zoals deze staat beschreven op de vorige pagina.

Als u nog verdere informatie over het onderzoek zou willen krijgen kunt u zich wenden tot de verantwoordelijke onderzoeker, Dr. Joanna Strycharz, email j.strycharz@uva.nl, Nieuwe Achtergracht 166, 1001 NG Amsterdam.

Mochten er naar aanleiding van uw deelname aan dit onderzoek bij u klachten of opmerkingen zijn, dan kunt u contact opnemen met het lid van de Commissie Ethiek namens de Amsterdam School of Communication Research, per adres:

ASCoR Secretariat,
Ethics Committee,
University of Amsterdam,
PO Box 15793,
1001 NG Amsterdam;
020-525 3680;
ascor-secr-fmg@uva.nl.

Een vertrouwelijke behandeling van uw klacht of opmerking is daarbij gewaarborgd.

____

[DEELNEMER]
- Ik ben 16 jaar of ouder.
- Ik heb de informatie gelezen en begrepen.
- Ik stem toe met deelname aan het onderzoek en gebruik van de daarmee verkregen gegevens.
- Ik behoud het recht om zonder opgaaf van reden deze instemming weer in te trekken binnen 7 dagen na afloop van dit onderzoek.
- Als mijn onderzoeksresultaten gebruikt worden in wetenschappelijke publicaties, of op een andere manier openbaar worden gemaakt, dan zal dit volledig geanonimiseerd gebeuren. Mijn persoonsgegevens worden niet door derden ingezien zonder mijn uitdrukkelijke toestemming.
- Ik behoud het recht op ieder door mij gewenst moment te stoppen met het onderzoek.

[CONS]
1 = akoord 2 = niet akkoord

BLOCK: TECHNOLOGY USE AND ADOPTION

Intro
Wij willen graa g uw mening weten over specifieke digitale technologieën die worden ingezet om de verspreiding van corona tegen te gaan.

[APP_AWE]
De overheid heeft een app ontwikkeld die u waarschuwt als u in de buurt bent geweest van iemand die later positief is getest op het coronavirus. Deze app heet *CoronaMelder* en wordt momenteel in enkele regio's getest.

Was u op de hoogte van deze app voordat u deelnam aan deze studie?

1 = Ja   2 = Nee

[APP_WORK]
Hoe stelt u zich de werking van de CoronaMelder app voor?

Open

[APP_INSTAL]
Heeft u de CoronaMelder app geïnstalleerd op uw telefoon?

1 = Ja   2 = Nee   3 = Weet ik niet

Routing: Als 1 ->

[APP_ACTIVE]
Heeft u de CoronaMelder app geactiveerd (door de Bluetooth-verbinding te activeren)?

1 = Ja   2 = Nee   3 = Weet ik niet

[FEEL_APP]
Als de CoronaMelder app geïnstalleerd is op uw telefoon, in welke mate voelt u zich dan:

FEEL_APP1 verontrust?
FEEL_APP2 schuldig?
FEEL_APP3 trots?
FEEL_APP4 alert?
FEEL_APP5 beschaamd?
FEEL_APP6 nerveus?
FEEL_APP7 bang?

1. Helemaal niet – 7. Helemaal wel\

[APP_ATT]
Over het algemeen hoe beoordeelt u de CoronaMelder app?

APP_ATT1 1. Slecht – 7. Goed
APP_ATT2 1. Schadelijk – 7. Gunstig

APP_ATT3 1. Onaangenaam – 7. Aangenaam
APP_ATT4 1. Waardeloos – 7. Waardevol

____

[APP_EX]
Kunt u uw ervaring met de CoronaMelder app kort beschrijven?

Open

____

[WITH_APP]
U heeft de CoronaMelder app heeft geïnstalleerd. In hoeverre bent u van plan om:

WITH_APP1 Als u positief getest wordt, een positief resultaat van de coronatest door te geven?
WITH_APP2 Bluetooth uit te zetten zodat de app geen gegevens kan uitwisselen?
WITH_APP3 Uw telefoon in de publieke ruimte uit te zetten (bijv. in een restaurant)?

1. Helemaal niet – 7. Helemaal wel

Routing: Als 2 ->

____

[FEEL_NOAPP]
Stelt u zich voor dat u de CoronaMelder app zou instaleren. In welke mate zou u zich dan _____ voelen:

FEEL_NOAPP1 verontrust
FEEL_NOAPP2 schuldig
FEEL_NOAPP3 trots
FEEL_NOAPP4 alert
FEEL_NOAPP5 beschaamd
FEEL_NOAPP6 nerveus
FEEL_NOAPP7 bang

1. Helemaal niet - 7. Helemaal wel

____

[WITH_NOAPP]
Stelt u zich voor dat u de CoronaMelder app heeft geïnstalleerd. Zou u:

WITH_NOAPP1 Een positief resultaat van de coronatest doorgeven?
WITH_NOAPP2 Bluetooth uitzetten zodat de app geen gegevens kan uitwisselen?
WITH_NOAPP3 Uw telefoon in de publieke ruimte uitzetten (bijv. in een restaurant)?

1 = Ja 2 = Nee 3 = Weet ik niet

Einde routing

____

[TELECOM_AWE]

De overheid wil geanonimiseerde locatiegegevens van uw mobiele telefoon gebruiken om bij te kunnen houden hoe het coronavirus zich verspreidt en op welke plekken er een groter risico op besmetting is.

Was u op de hoogte van het gebruik van anonieme locatiegegevens voordat u deelnam aan deze studie?

1 = Ja 2 = Nee

[MOTIV]
In hoeverre bent u gemotiveerd om:

MOTIV1 De eerdergenoemde CoronaMelder app op uw mobiele telefoon te installeren.
MOTIV2 De overheid toestemming te geven om geanonimiseerde locatiegegevens van uw telefoon te gebruiken.

1. Helemaal niet – 7. Helemaal wel

[APP_MOTIV]
Stelt u zich voor dat de overheid de CoronaMelder app in heel Nederland beschikbaar maakt. In hoeverre zou u gegevens over besmetting willen delen via de contact-tracing app?

APP_MOTIV1 In hoeverre bent u bereid om uw gegevens te delen via de contact-tracing app?

1. Zeer onbereid - 7. Zeer bereid

APP_MOTIV2 Hoe aannemelijk is het dat u uw gegevens zou delen via de contact-tracing app?

1. Zeer onaannemelijk - 7. Zeer aannemelijk

[ACCEPT]
In hoeverre vindt u de onderstaande manieren acceptabel om de verspreiding van de ziekte tegen te houden?

ACCEPT2 Het gebruik van apps om bij te houden wanneer je in de buurt bent geweest van iemand die besmet is.
ACCEPT3 Het gebruik geanonimiseerde locatiegevevens van mobiele telefoons om mensen te volgen die mogelijk besmettelijk zijn.

1. Helemaal niet acceptabel - 7. Helemaal wel acceptabel
9. Weet ik niet

BLOCK: INDIVIDUELE KENMERKEN

[NORM]
In hoeverre bent u het eens met de volgende stellingen?

U kunt bij deze stellingen dan een inschatting maken van wat u zou vinden als u gebruik zou maken van de contact-tracing app.

NORM1 De meeste van mijn vrienden vinden dat ik de CoronaMelder app moet gebruiken.
NORM2 De meeste van mijn familie vinden dat ik de CoronaMelder app moet gebruiken.
NORM3 Mijn partner vindt dat ik de CoronaMelder app moet gebruiken.
NORM4 Mijn werkgever vindt dat ik de CoronaMelder app moet gebruiken.
NORM5 De meeste mensen die ik ken vinden dat ik de CoronaMelder app moet gebruiken.
NORM6 De meeste van mijn vrienden zouden de CoronaMelder app installeren.
NORM7 De meeste van mijn familie zouden de CoronaMelder app installeren
NORM8 Mijn partner zou de CoronaMelder app installeren.
NORM9 De meeste mensen die ik ken zouden de CoronaMelder app installeren.

1. Helemaal mee oneens - 7. Helemaal mee eens
9. Niet van toepassing

____

[TRST]
Nu volgen enkele stellingen over het vertrouwen dat u persoonlijk heeft in de volgende instellingen. Zou u voor elk van de volgende stellingen kunnen aangeven in hoeverre u het ermee eens of oneens bent?

TRST1 Ik vertrouw de Tweede Kamer.
TRST2 Ik vertrouw politici.
TRST3 Ik vertrouw politieke partijen.
TRST4 Ik vertrouw het rechtssysteem.
TRST5 Ik vertrouw de politie.
TRST6 Ik vertrouw de regering.
TRST7 Ik vertrouw de Europese Unie.
TRST8 Ik vertrouw de RIVM.

1. Helemaal mee oneens - 7. Helemaal mee eens

____

[TRUST_GOV]
In hoeverre bent u het eens of oneens met de volgende stellingen?

TRUST_GOV1 De overheid is betrouwbaar in het behandelen van mijn persoonlijke data
TRUST_GOV2 Ik vertrouw erop dat de overheid goed met mijn persoonlijke data omgaat
TRUST_GOV3 De overheid is eerlijk als het gaat om het gebruik van mijn persoonlijke data

1. Helemaal mee oneens - 7. Helemaal mee eens

____

[RISK_GOV]
In hoeverre bent u het eens of oneens met de volgende stellingen?

RISK_GOV1 In het algemeen is het riskant om mijn persoonlijke data aan de overheid

te geven
RISK_GOV2 Ik verlies mijn privacy als ik mijn persoonlijke data aan de overheid verstrek
RISK_GOV 3Er is te veel onzekerheid bij het geven van mijn persoonlijke data aan de overheid
RISK_GOV4 Persoonlijke gegevens die ik deel kunnen door de overheid voor andere doeleinden worden gebruikt.
RISK_GOV5 Ik voel me veilig om mijn persoonlijke data af te staan aan de overheid

1. Helemaal mee oneens - 7. Helemaal mee eens

[TRUST_TECH]
In hoeverre bent u het oneens of eens met de volgende stellingen?

TRUST_TECH1 Techbedrijven zoals Google of Apple zijn betrouwbaar in het behandelen van mijn persoonlijke data
TRUST_TECH2 Ik vertrouw erop dat techbedrijven zoals Google of Apple mijn persoonlijke data te goeder trouw behandelen
TRUST_TECH3 Techbedrijven zoals Google of Apple zijn eerlijk als het gaat om het gebruik van mijn persoonlijke data.
TRUST_TECH4 Ik geloof dat techbedrijven zoals Google of Apple in mijn beste belang handelen.
TRUST_TECH5 Als ik hulp zou nodig hebben, zouden techbedrijven zoals Google of Apple hun best doen om mij te helpen.
TRUST_TECH6 Techbedrijven zoals Google of Apple zijn geïnteresseerd in mijn welzijn, niet alleen in hun eigen welzijn

1. Helemaal mee oneens - 7. Helemaal mee eens

[RISK_TECH]

RISK_TECH1 In het algemeen is het riskant zijn om mijn persoonlijke data aan techbedrijven zoals Google of Apple te geven
RISK_TECH2 Ik verlies mijn privacy als ik mijn persoonlijke data aan techbedrijven zoals Google of Apple verstrekt
RISK_TECH3 Er is te veel onzekerheid bij het geven van mijn persoonlijke data aan techbedrijven zoals Google of Apple
RISK_TECH4 Persoonlijke gegevens die ik deel kunnen voor andere doeleinden worden gebruikt.
RISK_TECH5 Ik voel me veilig om mijn persoonlijke data af te staan aan techbedrijven zoals Google of Apple

1. Helemaal mee oneens - 7. Helemaal mee eens

[RISK_SAMEN]
Voor de CoronaMelder app werkt de Nederlandse overheid samen met Google en Apple zodat de CoronaMelder app beschikbaar kan zijn op de smartphone. In hoeverre bent u het oneens of eens met de volgende stellingen?

RISK_SAMEN1 In het algemeen is het riskant als de overheid met Google en Apple samenwerkt.
RISK_SAMEN2 Ik verlies mijn privacy als de overheid met Google of Apple samenwerkt
RISK_SAMEN3 Er is te veel onzekerheid bij de samenwerking van de overheid met Google en Apple.
RISK_SAMEN4 De samenwerking kan voor andere doeleinden worden gebruikt dan de CoronaMelder app.
RISK_SAMEN5 Ik voel me veilig bij een samenwerking tussen de overheid en Google en Apple
RISK_SAMEN6 De Nederlandse overheid maakt zich te afhankelijk van Google en Apple.
RISK_SAMEN7 Door de samenwerking word ik afhankelijk van Google en Apple.
1. Helemaal mee oneens – 7. Helemaal mee eens

[WOM]
In hoeverre bent u het oneens of eens met de volgende stellingen?

WOM1 Ik zal mijn vrienden en familie aanmoedigen om de CoronaMelder app te instaleren.
WOM2 Ik zal me positief over de CoronaMelder app uiten.
WOM3 Ik zal positieve dingen over de CoronaMelder app zeggen.
WOM4 Ik zal de CoronaMelder app van harte aan andere aanbleven.

1. Helemaal mee oneens - 7. Helemaal mee eens

[INTAPP]
Stelt u voor dat u de CoronaMelder app gebruikt en u een melding krijgt in de app dat u in contact bent geweest met een besmette persoon. U wordt geadviseerd om tot 10 dagen na de datum van het contact met een besmette persoon thuis te blijven. In hoeverre bent u het oneens of eens met de volgende stellingen over dit advies?

INTAPP1 Ik zou nerveus zijn om actie te ondernemen naar aanleiding van het advies van de app.
INTAPP2 Ik zou me zorgen maken om het advies van de app te volgen.
INTAPP3 Ik zou me ongemakkelijk voelen om het advies van de app te volgen.
INTAPP4 Onlangs het advies van de app zou ik niet thuisblijven.

1. Helemaal mee oneens - 7. Helemaal mee eens

[VOTE]
Op welke partij zou u stemmen als er morgen in Nederland verkiezingen voor de Tweede Kamer zouden worden gehouden?

VOTE1 VVD
VOTE2 PVV
VOTE3 D66
VOTE4 GL
VOTE5 PvdA
VOTE6 CU
VOTE7 SGP

VOTE8 DENK
VOTE9 FvD
VOTE10 50+
VOTE11 PvdT
VOTE12 Andere partij, namelijk: *open*
VOTE13 Weet ik niet
VOTE14 Ik zou niet stemmen
VOTE15 Blanco

[VALUE]
In onze maatschappij spelen digitale technologieën en kunstmatige intelligentie in toenemende mate een grote rol. Hoe belangrijk zijn de volgende waarden en overwegingen voor u als de overheid regelgeving hierover opstelt?

VALUE1 Rechtvaardigheid van de technologische toepassing
VALUE2 Gelijkheid tussen burgers beïnvloed door de technologische toepassing
VALUE3 Diversiteit in de aanbevelingen van de technologische toepassing
VALUE4 Duidelijkheid wie verantwoordelijk is voor de technologische toepassing
VALUE5 Transparantie hoe kunstmatige intelligentie toegepast wordt
VALUE6 Invloed op samenhang in de samenleving
VALUE7 Betrouwbarheid van de technologische toepassing
VALUE8 Solidariteit tussen burgers
VALUE9 Respect voor privacy van burgers
VALUE10 Democratische controle

1 Helemaal niet belangrijk - 7. Heel erg belangrijk

Routing: Sample opsplitsen in drie delen

[VALOP1]
Als u aan het gebruik van digitale technologieën en kunstmatige intelligentie binnen de rechtspraak denkt, welke waarden zijn dan voor u belangrijk?

Open

[VALOP2]
Als u aan het gebruik van digitale technologieën en kunstmatige intelligentie binnen de gezondheidszorg denkt, welke waarden zijn dan voor u belangrijk?

Open

[VALOP3]
Als u aan het gebruik van digitale technologieën en kunstmatige intelligentie binnen de media denkt, welke waarden zijn dan voor u belangrijk?

Open

Survey Wave 3: Codebook

INFORMATIEBROCHURE VOOR DEELNEMERS AAN ONDERZOEK
"Technologie en samenleving"

Beste deelnemer,

Dit onderzoek voeren we uit in opdracht van de Universiteit van Amsterdam (UvA). Voordat u aan het onderzoek begint, wil de UvA u een aantal zaken laten weten. Het is belangrijk dat u op de hoogte bent van de procedure die in dit onderzoek wordt gevolgd. Lees daarom onderstaande tekst alstublieft zorgvuldig door en aarzel niet om opheldering te vragen over de tekst. De UvA-onderzoekers beantwoorden eventuele vragen graag.

Doel van het onderzoek

In deze vragenlijst wordt naar uw mening over technologie en de samenleving gevraagd. Het doel van dit onderzoek is om het gedrag en de opvattingen van Nederlanders ten opzichte van dit onderwerp beter te begrijpen. We zullen u in de toekomst nog tweemaal uitnodigen voor een korte vragenlijst over technologie en de samenleving.

Gang van zaken tijdens het onderzoek

Als u akkoord gaat met deelname aan dit onderzoek, zal u een aantal vragen over technologie en de samenleving krijgen in de huidige coronacrisis. De vragenlijst duurt ongeveer 15 minuten.

Vertrouwelijkheid van gegevens

Uw persoonsgegevens (persoonlijke informatie) blijven vertrouwelijk en worden niet gedeeld met anderen zonder uw uitdrukkelijke toestemming. De onderzoeksgegevens worden voor wetenschappelijk onderzoek geanalyseerd door de onderzoekers van dit project. De onderzoeksresultaten worden gebruikt in wetenschappelijke publicaties. De data zullen daarvoor openbaar worden gemaakt, maar dit zal volledig geanonimiseerd gebeuren.

Vrijwilligheid

U kunt uw medewerking ten alle tijden staken zonder opgave van redenen. Tevens kunt u zeven dagen na dit onderzoek alsnog uw toestemming intrekken. Mocht u uw medewerking nu staken of achteraf uw toestemming intrekken, dan zullen uw gegevens worden verwijderd uit onze bestanden en vernietigd.

TOESTEMMINGSVERKLARING

Als u akkoord gaat, verklaart u dat u de deelnemersinformatie heeft gelezen en begrepen. Verder geeft u met de ondertekening te kennen dat u akkoord gaat met de gang van zaken zoals deze staat beschreven op de vorige pagina.

Als u nog verdere informatie over het onderzoek zou willen krijgen kunt u zich wenden tot de verantwoordelijke onderzoeker, Dr. Joanna Strycharz, email j.strycharz@uva.nl, Nieuwe Achtergracht 166, 1001 NG Amsterdam.

Mochten er naar aanleiding van uw deelname aan dit onderzoek bij u klachten of opmerkingen zijn, dan kunt u contact opnemen met het lid van de Commissie Ethiek namens de Amsterdam School of Communication Research, per adres:

ASCoR Secretariat,
Ethics Committee,
University of Amsterdam,
PO Box 15793,
1001 NG Amsterdam;
020-525 3680;
ascor-secr-fmg@uva.nl.

Een vertrouwelijke behandeling van uw klacht of opmerking is daarbij gewaarborgd.

[DEELNEMER]

- Ik ben 16 jaar of ouder.
- Ik heb de informatie gelezen en begrepen.
- Ik stem toe met deelname aan het onderzoek en gebruik van de daarmee verkregen gegevens.
- Ik behoud het recht om zonder opgaaf van reden deze instemming weer in te trekken binnen 7 dagen na afloop van dit onderzoek.
- Als mijn onderzoeksresultaten gebruikt worden in wetenschappelijke publicaties, of op een andere manier openbaar worden gemaakt, dan zal dit volledig geanonimiseerd gebeuren. Mijn persoonsgegevens worden niet door derden ingezien zonder mijn uitdrukkelijke toestemming.
- Ik behoud het recht op ieder door mij gewenst moment te stoppen met het onderzoek.

[CONS]

1 = akkoord 2 = niet akkoord

BLOCK: TECHNOLOGY USE, ADOPTION AND PERCEPTIONS

Intro
Wij willen graag uw mening weten over specifieke digitale technologieën die worden ingezet om de verspreiding van corona tegen te gaan.

***RM:* Awareness of contact tracing app**
De overheid heeft een app ontwikkeld die u waarschuwt als u in de buurt bent geweest van iemand die later positief is getest op het coronavirus. Deze app heet *Corona-Melder.*

Was u op de hoogte van deze app voordat u deelnam aan deze studie?

1 = Ja 2 = Nee

***RM:* Installation of contact tracing app**
Heeft u de CoronaMelder-app op uw telefoon geïnstalleerd?

1 = Ja 2 = Nee 3 = Weet ik niet

Routing: Als 1 à

***RM:* App activation**
Heeft u de CoronaMelder-app geactiveerd (door de Bluetooth-verbinding te activeren)?

1 = Ja 2 = Nee 3 = Weet ik niet

***RM:* Attitude towards the app**
Over het algemeen hoe beoordeelt u de CoronaMelder-app?

APP_ATT1 1. Slecht – 7. Goed
APP_ATT2 1. Schadelijk – 7. Gunstig
APP_ATT3 1. Onaangenaam – 7. Aangenaam
APP_ATT4 1. Waardeloos – 7. Waardevol

***RM:* Experiences with the app**
Kunt u uw ervaring met de CoronaMelder-app kort beschrijven?

Open

***RM:* Self-disclosure and withdrawal intention**
U heeft de CoronaMelder-app geïnstalleerd. In hoeverre bent u van plan om:

WITH_APP1 Een positief testresultaat via de app door te geven om andere mensen te waarschuwen?
WITH_APP2 Af en toe Bluetooth uit te zetten zodat de app geen gegevens kan uitwisselen?
WITH_APP3 Uw telefoon in de publieke ruimte uit te zetten (bijv. in een restaurant)?
WITH_APP4 De app van uw telefoon verwijderen.

1. Helemaal niet – 7. Helemaal wel

Als 2 ->

***RM:* Motivation to use/install**
In hoeverre bent u gemotiveerd om:

MOTIV1 De eerdergenoemde CoronaMelder-app op uw mobiele telefoon te installeren.

1. Helemaal niet – 7. Helemaal wel

***RM:* Self-disclosure and withdrawal intention**
Stelt u zich voor dat u de CoronaMelder-app heeft geïnstalleerd. Zou u:

WITH_NOAPP1 Een positief testresultaat via de app doorgeven om andere mensen te waarschuwen?
WITH_NOAPP2 Af en toe Bluetooth uitzetten zodat de app geen gegevens kan uitwisselen?
WITH_NOAPP3 Uw telefoon in de publieke ruimte uitzetten (bijv. in een restaurant)?

1 = Ja 2 = Nee 3 = Weet ik niet

Einde routing

***RM:* Awareness of telecom data**
De overheid wil geanonimiseerde locatiegegevens van uw mobiele telefoon gebruiken om bij te kunnen houden hoe het coronavirus zich verspreidt en op welke plekken er een groter risico op besmetting is.

Was u op de hoogte van het gebruik van anonieme locatiegegevens voordat u deelnam aan deze studie?

1 = Ja 2 = Nee

***RM:* Acceptance**
In hoeverre vindt u de onderstaande manieren acceptabel om de verspreiding van de ziekte tegen te houden?

ACCEPT2 Het gebruik van apps om bij te houden wanneer je in de buurt bent geweest van iemand die besmet is.

ACCEPT3 Het gebruik van geanonimiseerde locatiegegevens van mobiele telefoons om inzicht te krijgen in hoe groepen mensen zich bewegen en het virus zich verspreidt.

1. Helemaal niet acceptabel – 7. Helemaal wel acceptabel
9. Weet ik niet

Information quality about app
De volgende vragen gaan over informatie over de contact-tracing app CoronaMelder die u bent tegengekomen. In hoeverre bent u het eens met de volgende stellingen?

INFO1 Ik ben voldoende geïnformeerd over de werking van de contact-tracing app.
INFO2 Ik ben voldoende geïnformeerd over welke data de contact-tracing app verzamelt.
INFO3 Ik ben voldoende geïnformeerd om gebruik te kunnen maken van de contact-tracing app.
INFO4 Ik ben voldoende geïnformeerd over de gevolgen voor mij als ik de contact-tracing app installeer.
INFO5 Ik ben voldoende geïnformeerd over de gevolgen voor mij als ik een melding via de contact-tracing app krijg.

1. Helemaal mee oneens - 7. Helemaal mee eens

***RM:* Intention to follow app’s advice**
Stelt u voor dat u de CoronaMelder-app gebruikt en u een melding krijgt in de app dat u in contact bent geweest met een besmet persoon. U wordt geadviseerd om tot 10 dagen na de datum van het contact met een besmet persoon thuis te blijven. In hoeverre bent u het oneens of eens met de volgende stellingen over dit advies?

INTAPP1 Ik zou nerveus zijn om actie te ondernemen naar aanleiding van het advies van de app.
INTAPP2 Ik zou me zorgen maken om het advies van de app te volgen.
INTAPP3 Ik zou me ongemakkelijk voelen om het advies van de app te volgen.
INTAPP4 Ondanks het advies van de app zou ik niet thuisblijven.
INTAPP5 Ik zou me 5 dagen na de melding laten testen als ik geen klachten hebt.

1. Helemaal mee oneens - 7. Helemaal mee eens

Perceived benefits of contact tracing apps
De volgende vragen gaan over uw mening over de CoronaMelder-app. In hoeverre bent u het eens met de volgende stellingen?

PB1 Gebruikers van de CoronaMelder-app dragen bij aan het beperken van de verspreiding van het coronavirus.
PB2 Gebruikers van de CoronaMelder-app dragen bij aan eigen gezondheid.
PB3 Gebruikers van de CoronaMelder-app dragen bij aan gezondheidszorg in het

algemeen.
PB4 Gebruik van de app leidt tot betere naleving van de huidige coronaregels (zoals social distancing of hygiëne)
PB5 Gebruikers van de app beschermen mensen in hun directe omgeving.
PB6 Gebruikers van de app dragen bij aan betere bescherming voor kwetsbare groepen in de maatschappij.
PB7 Gebruik van de CoronaMelder-app is voordelig omdat gebruikers zich sneller kunnen laten testen.
PB8 Gebruik van de CoronaMelder-app is voordelig omdat gebruikers informatie over contact met een besmet persoon kunnen krijgen.
PB9 Gebruik van de CoronaMelder-app draagt bij aan het voorkomen van een lockdown.

1. Helemaal mee oneens -7. Helemaal mee eens

____

Privacy concerns
Er volgt nu een aantal specifieke stellingen over gebruik van de contact-tracing app CoronaMelder. Geef voor iedere stelling aan of u het hiermee oneens of eens bent.

PRIV_CON1 Ik ben bezorgd dat gegevens verzameld via de CoronaMelder-app misbruikt kunnen worden door anderen wanneer ik de contact-tracing app gebruik.
PRIV_CON2 Wanneer ik de CoronaMelder-app gebruik heb ik het gevoel dat anderen mijn locatie kunnen bijhouden.
PRIV_CON3 Ik ben bang dat mijn gegevens verzameld via de CoronaMelder-app niet veilig worden opgeslagen.
PRIV_CON4 Ik ben bezorgd dat gegevens verzameld via de CoronaMelder-app verder worden verspreid naar andere partijen.
PRIV_CON5 Ik ben bezorgd dat gegevens verzameld via de CoronaMelder-app gezien of gehoord worden door mensen die ik niet ken.
PRIV_CON6 Ik ben bang dat gegevens verzameld via de CoronaMelder-app voor andere doeleinden worden gebruikt.
PRIV_CON7 Ik ben bezorgd dat ik geen controle heb over wie mijn gegevens verzameld via de CoronaMelder-app kan inzien.

1 Helemaal mee oneens - 7. Helemaal mee eens

____

Other concerns (based on open answers)
De volgende vragen gaan over uw mening over de CoronaMelder-app. In hoeverre bent u het eens met de volgende stellingen?

OTHER_CON1 Ik ben bang dat gebruik van de CoronaMelder-app een negatieve invloed zou hebben op de werking van mijn mobiele telefoon.
OTHER_CON2 Ik maak me zorgen dat niet iedereen de nodige middelen heeft om de CoronaMelder-app te kunnen gebruiken (bijv. een smartphone).
OTHER_CON3 Ik ben bezorgd dat de CoronaMelder-app misbruikt kan worden door fraudeurs.
OTHER_CON4 Ik ben bezorgd dat de CoronaMelder-app voor spanningen zorgt tussen personen die besmet zijn met het coronavirus en degenen die dat niet zijn.
OTHER_CON5 Ik ben bezorgd dat het gebruik van de CoronaMelder-app ertoe kan leiden

dat mensen ongelijk behandeld worden.
OTHER_CON6 Ik ben bang dat andere mensen in de directe omgeving kunnen achterhalen dat de CoronaMelder-app-gebruiker besmet is.
OTHER_CON7 Ik maak me zorgen over de quarantaineplicht na een melding door de CoronaMelder-app.
OTHER_CON8 Ik ben bang dat als ik de CoronaMelder-app installeer, ik hem niet meer kan verwijderen.
OTHER_CON9 Ik ben bang dat de CoronaMelder-app in de toekomst voor andere doelen gebruikt kan worden.
OTHER_CON10 Ik ben bang dat de CoronaMelder-app door de overheid gebruikt kan worden om mensen beter in de gaten te houden.
OTHER_CON11 Ik ben bang dat de CoronaMelder-app door grote techbedrijven zoals Google en Apple gebruikt kan worden om meer data over mij te verzamelen.
OTHER_CON12 Ik ben bang dat de Nederlandse overheid te afhankelijk wordt van grote techbedrijven zoals Google en Apple.

1. Helemaal mee oneens - 7. Helemaal mee eens

BLOCK: INDIVIDUAL VULNERABILITY FACTORS

Work situation 1
Heeft u op dit moment betaald werk als werknemer?

(Ook 1 uur per week of een korte periode telt al mee.)

1. Ja 2. Nee

Als 1:

Work situation 2
We willen graag meer weten over uw werkomstandigheden.

Als u meerdere banen heeft, vul de vraag in voor de baan waar u gemiddeld de meeste tijd aan besteedt.

Wat is uw huidige werksituatie?

1. werknemer met vast contract en vaste uren
2. werknemer met nulurencontract
3. werknemer met tijdelijk contract met uitzicht op vast contract
4. werknemer tijdelijk contract van langer dan 1 jaar
5. werknemer tijdelijk contract van korter dan 1 jaar

6. oproep/-invalkracht
7. uitzendkracht
8. werkzaam via de WSW (Wet Sociale Werkvoorziening) of Participatiewet
8. werkzaam als zelfstandige

Als [3, 4, 5, 6, 7]:

Reason flexible work
Wat is de belangrijkste reden waarom u op dit moment flexibel werk heeft?

1. Ik heb behoefte aan flexibiliteit
2. Ik ben nieuw bij mijn huidige werkgever
3. Er is geen vaste baan beschikbaar voor mij
4. Anders [*open*]

Work location pre-corona
Op welke locatie werkte u voor de coronapandemie doorgaans voor uw werkgever?

1. Op mijn eigen woonadres
2. Op een vast adres van uw werkgever
3. Op verschillende plaatsen

Work location corona
Op welke locatie werkt u *nu*, tijdens coronapandemie, doorgaans voor uw werkgever?

1. Op mijn eigen woonadres
2. Op een vast adres van uw werkgever
3. Op verschillende plaatsen

Work sector
De volgende vragen gaan over het bedrijf / de instelling waar u op dit moment werkt.

Om wat voor soort bedrijf of instelling gaat het?

1. Productiebedrijf / Fabriek
2. Bouwbedrijf
3. Transport- of vervoersbedrijf
4. (Web)Winkel / Groothandel / Marktkraam
5. Horecagelegenheid
6. Gezondheids- of zorginstelling
7. Onderwijsinstelling
8. Overheidsinstelling
9. Financiële instelling
10. ICT-bedrijf

11. Particulier huishouden
12. Anders *[open]*

Beroep
De volgende vragen gaan over uw beroep.

Welk beroep of welke functie oefent u uit?

Probeer in de omschrijving zo specifiek mogelijk te zijn, bijvoorbeeld door een specialisme of niveau op te geven

Open

Emotional states
We willen graag weten hoe u zich de afgelopen week heeft gevoeld naar aanleiding van de voorzorgsmaatregelen rondom het coronavirus. In hoeverre bent u het oneens of eens met de volgende stellingen?

In de afgelopen 7 dagen voelde ik me:

EMOSTATES1 Angstig
EMOSTATES2 Van streek
EMOSTATES3 Nerveus
EMOSTATES4 Bang
EMOSTATES5 Alert
EMOSTATES6 Sterk
EMOSTATES7 Vastbesloten
EMOSTATES8 Oplettend

1. Nauwelijks of helemaal niet
2. Een beetje
3. Gemiddeld
4. Nogal
5. In sterke mate

***RM:* Injunctive and descriptive norm**
De volgende stellingen gaan over uw gebruik van de CoronaMelder-app

In hoeverre bent u het eens met de volgende stellingen?

NORM1 De meeste van mijn vrienden vinden dat ik de CoronaMelder-app moet gebruiken.
NORM2 De meeste van mijn familie vinden dat ik de CoronaMelder-app moet gebruiken.
NORM3 Mijn partner vindt dat ik de CoronaMelder-app moet gebruiken.
NORM4 Mijn werkgever vindt dat ik de CoronaMelder-app moet gebruiken.
NORM5 De meeste mensen die ik ken vinden dat ik de CoronaMelder-app moet gebruiken.
NORM6 De meeste van mijn vrienden zouden de CoronaMelder-app installeren.
NORM7 De meeste van mijn familie zouden de CoronaMelder-app installeren
NORM8 Mijn partner zou de CoronaMelder-app installeren.

NORM9 De meeste mensen die ik ken zouden de CoronaMelder-app installeren.

1. Helemaal mee oneens - 7. Helemaal mee eens

____

Perceived voluntariness
De volgende vragen gaan over uw waarneming rondom de CoronaMelder-app.

In hoeverre bent u het oneens of eens met de volgende stellingen over deze app?

PVOL1 De overheid verwacht dat ik de app gebruik.
PVOL2 Mijn werkgever verwacht dat ik de app gebruik.
PVOL3 Mijn werkgever wil niet dat ik de app gebruik.
PVOL4 Mijn gebruik van de app is geheel vrijwillig
PVOL5 Hoewel het nuttig kan zijn, is het gebruik van de app zeker niet verplicht.
PVOL6 Ik vrees negatieve gevolgen voor mijn privéleven als ik de app niet gebruik.
PVOL7 Ik vrees negatieve gevolgen voor mijn werk als ik de app niet gebruik.

1. Helemaal mee oneens - 7. Helemaal mee eens

____

Moral obligation
In hoeverre bent u het oneens of eens met de volgende stelling?

MO1 Ik ben het moreel verplicht om de CoronaMelder-app te instaleren.

1. Helemaal mee oneens - 7. Helemaal mee eens

____

Normative obligation to obey the authorities (Posch et al. 2020)
De volgende vragen gaan over de manier waarop de overheid het coronavirus bestrijdt.

In hoeverre bent u het oneens of eens met de volgende stellingen?

NO1 Ik voel een morele verplichting om de maatregelen van de overheid om het coronavirus te bestrijden op te volgen.
NO2 Ik voel een morele plicht om de maatregelen van de overheid om het coronavirus te bestrijden te steunen, zelfs als ik het niet met de maatregelen eens ben.
NO3 Ik voel een morele plicht om de maatregelen van de overheid om het coronavirus te bestrijden op te volgen, zelfs als ik de redenen erachter niet begrijp.

1. Helemaal mee oneens - 7. Helemaal mee eens

____

Non-normative obligation to obey the authorities
In hoeverre bent u het oneens of eens met de volgende stellingen?

NNO1 Mensen zoals ik hebben geen andere keuze dan de maatregelen van de overheid om het coronavirus te bestrijden op te volgen.
NNO2 Ik volg de maatregelen van de overheid om het coronavirus te bestrijden alleen omdat ik bang ben voor de overheid.

NNO3 Als je de maatregelen van de overheid om het coronavirus te bestrijden niet opvolgt, zal het negatieve consequenties hebben.

1. Helemaal mee oneens - 7. Helemaal mee eens

Cost of app

Stelt u voor dat u de CoronaMelder-app gebruikt en u een melding krijgt in de app dat u in contact bent geweest met een besmet persoon. U wordt geadviseerd om tot 10 dagen na de datum van het contact met een besmet persoon thuis te blijven. Hoe waarschijnlijk is het dat u in deze situatie:

COST1 uw inkomen zou verliezen
COST2 uw baan zou verliezen
COST3 niet zou kunnen werken
COST4 niet zo effectief zou kunnen werken als normaal
COST5 een negatieve impact zou ervaren op uw sociale leven

1. Helemaal niet waarschijnlijk – 7. Zeer waarschijnlijk

Awareness CoronaMelder-wet

De Tijdelijke wet notificatieapplicatie covid-19 bevat regels voor de CoronaMelder-app. De wet zegt dat niemand mag worden verplicht om de app te installeren, en de wet bevat nog meer regels over het gebruik van persoonlijke gegevens en de beveiliging van de gegevens.

Was u op de hoogte van deze wet voordat u deelnam aan deze studie?

1 = Ja 2 = Nee

Institutional trust in law

In hoeverre bent u het eens met de volgende stellingen?

IT1 De huidige wetten bieden mij genoeg bescherming om mij het vertrouwen te geven dat ik de CoronaMelder-app kan installeren
IT2 Ik voel mij ervan verzekerd dat mijn rechten adequaat beschermd worden door de huidige wetten.
IT3 Ik heb er vertrouwen in dat de huidige wetten het veilig maken om de CoronaMelder-app te gebruiken
IT4 De huidige wetten zorgen over het algemeen voor een robuuste en veilige omgeving om de CoronaMelder-app te installeren.
IT5 Ik heb vertrouwen in de Coronamelder-app omdat die wettelijk is geregeld.

1. Helemaal mee oneens - 7. Helemaal mee eens

IViR - Institute for Information Law
P.O. Box 15514, 1001 NA Amsterdam, the Netherlands

https://www.ivir.nl/