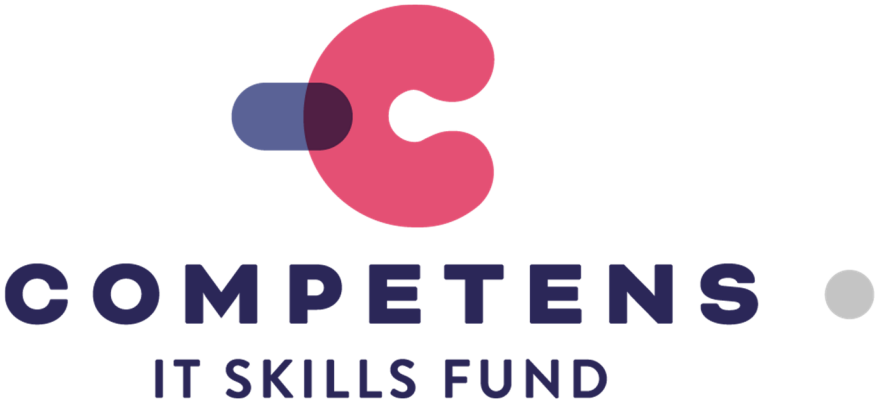
Multidisciplinary aspects of COVID-19 apps

Natascha van Duuren, Victor de Pous

Multidisciplinary Aspects of COVID-19 apps

Natascha van Duuren LLM
Victor de Pous LLM (eds.)

Multidisciplinary aspects of COVID-19 apps



The Competens Foundation, Skillsfund for IT, financed the translation of this publication. This foundation's mission is to support initiatives to strengthen IT skills for growth and innovation in the Netherlands. This publication adds to that mission, because it supports IT skills growth by sharing insights, experiences and best practices gained around developing COVID apps from a multidisciplinary perspective.

See: www.competens.nl

Multidisciplinary aspects of COVID-19 apps

Natascha van Duuren and
Victor de Pous (ed.)

ISBN: 978-90-9034977-0
NUR: 820

Contents

Foreword 9

Editorial 13

1 **COVID-19 apps as survey point for ICT and the digitalising society** 15
Victor de Pous

2 **The use(lessness) of digital contact tracing** 24
Gabrielle Speijer

3 **A different kind of antivirus: the technology and data logistics of contact-tracing apps** 32
Marco Bommeljé

4 **Germany: Great Expectations and a partially Disillusioning Reality** 43
Rainer Malaka and Rai Kannenberg

5 **Corona-appathon: Wunderkind or Total Loss?** 49
Serge Wallagh

6 **Strict European tendering rules, even in times of crisis?** 55
Menno de Wijs

7 **Network and information security: apps that are secure by design?** 61
Paul Oor

8 **Privacy and COVID-19 apps** 67
Jeroen van Helden

9 **South Africa's Approach to COVID-19 Data Collection and Contact Tracking** 74
Paula Kotzé

10 **Financial aspects of COVID-19 apps** 84
Klaas Brongers, Martin van de Berg

11 **Project 2.0: CoronaMelder** 90
Siewert van Otterloo

12 **(Mis)understanding open-source software** 97
Victor de Pous

13 **Humanity by design: quality approach for digitalization** 105
Leon Dohmen, Joan Baaijens and Liesbeth Ruoff

14 **The legal status of a coronavirus app under European law** 113
Natascha van Duuren

15 **Digital preparedness of the healthcare sector** 120
Gabrielle Speijer

16 **The Australian COVID-19 Tracing App Experience** 127
Anthony Wong

17 **European cooperation: cross-border data processing** 137
Dirk de Wit

18 **Confidence in sharing personal data** 145
Erik Beulen

19 **Medical apps and patient rights** 151
Bert Morsink

20 **Some Viewpoints on RadarCOVID in Spain** 158
Carlos Juiz

21 **Competition aspects of app stores** 164
Rob Ludding

22 **Towards a new blueprint for government automation projects?** 169
Wouter Brongeest

23 **Liability for insecure software code and poor functioning** 175
Natascha van Duuren / Victor de Pous

24 **The Integrated Information Support Systems for Infection Disease Management in Korea** 183
Jee-Lin Kim

25 **The importance of supervision on mobile applications** 188
Maarten Souw

26 **Ethics and contact-tracing apps: A Better Way Forward?** 194
David Cars, Liesbeth Ruoff

List of authors 200

Foreword

The coronavirus crisis and the myriad measures that accompanied it have cut like a knife through Dutch society. Political affiliation, educational level, religious background, social status, circles of acquaintances, families – across all the traditional categories, disagreements sometimes become heated. Opinions are divided on the reasons, the measures themselves and the effects, desirable (and quantified) or otherwise. Our society finds itself in an era in which history is being written; an era that will be a lasting memory for everyone going forward.

For professionals in information management, information provision and information technology that is no different. The discussion on how the perceived crisis should be tackled has, for information professionals as well, prompted conversation and debate and given rise to discourse on how the profession can and must contribute.

In the case of contact-tracing coronavirus apps, included in the package of measures being worked out by many governments worldwide, the discussion is taking place at multiple levels. What is interesting, for instance, is the way in which legislation and implementation have become engaged in a kind of dance. Without a legislative framework, there is no implementation, and without implementing acts, implementing organisations cannot put measures into effect, and consequently there is no application of that legislation. Before political resolutions are formalised and subsequently carried out, long(er) timelines usually need to be taken into account. In the case of the coronavirus app, the legislative framework (the emergency act) was worked out in parallel to the development of the app. A unique situation in the constitutional arena.

What is also extraordinary is the way in which the debate on ethics came to the fore in the measures surrounding the introduction of the app. Many have become accustomed to the fact that people voluntarily allow commercial organisations some access to their personal information, aside from how consciously people make that consideration. The fact that the government is now explicitly working with commercial parties that provide the necessary preconditions to allow the app to function, and will be able to subsequently monitor and check up on individual citizens, adds a different dimension for many.

This is precisely the discussion that should be conducted more often, and it is part of our professional organisation's theme of Smart Humanity. After all, ICT facilities can be used for both good and evil. While 23 million citizens in China are being denied the right to travel as a result of constant social monitoring and scoring, we can use the same technology to identify notorious troublemakers in large crowds on time. And is that prospect 'terrifying' or in fact 'nice and safe'? Is this a case of 'COVID-1984', to reference George Orwell, or should we in fact be grateful because it means we can attend a music concert in a secure, protected environment?

The way in which access to information has been shaped over the past months has also prompted discussion. In the Netherlands, for instance, the coronavirus app was developed publicly as much as possible. In dialogue with our surroundings, with experts, and using open code. The information from CBS, RIVM, Stichting NICE, Nivel and LCPS, for instance, is publicly accessible, and the provision of information from the government via www.rijksoverheid.nl is working overtime. But has that information in fact been informative, concise, directive or imperative? And how up to date and, above all, reliable (and therefore verifiable) is all of it? Especially since organisations like the WHO continue to update their standards *and* their information sources, which means that the substantive frameworks for an app may also change.

In addition to the effect of politics, the rule of law, ethical debates and the search for the right information, there is also discussion about the role of information professionals. Because if an app is to be built, that poses a challenge for many. Is it technically possible? Can it be done securely? Is privacy optimally safeguarded? Can it be made user-friendly? What do we do with the notifications? What do we require of citizens who receive a notification? And also: is the ICT facility robust enough to accommodate high volumes of users during peak times, in cities and in rural areas, and can it be installed and maintained on all possible versions of mobile devices that people carry with them? And what do we do if the emergency act is repealed at some point?

The Royal Association of Information Professionals (KNVI) is an organisation of individual professionals. In a society in which information plays an increasingly important role, it is the KNVI's deepest conviction that humanity has a duty to itself to get the best out of its own inventions for the benefit of humanity. In other words, information professionals create technology and help with the implementation of this technology. They are creators and users as well as educators. They facilitate other people and organisations in accessing information. People are therefore the

focus for the professional organisation: They must be supported in standing up to the successive waves that disrupt society, and the societal effects and ethical impact of these waves.

In short, all the issues mentioned above converge in the information professionals who play a role in COVID-19 apps and in the formulation and implementation of the measures that have been taken by government organisations over the past months. From a professional perspective, we not only contribute; we also have a duty to reflect on our work. In terms of content, based on facts and arguments.

The drastic events surrounding COVID-19 present an interesting occasion to consider the current state of the (global) community. A broad range of differences — medical, social, political, information technology-related, democratic, legal and more — arise from country to country. We are proud of the fact that KNVI's experts can place their vision and knowledge of COVID-19 apps in a broader context. This has given rise to a special, topical and relevant publication. This book therefore makes a contribution towards reflecting on and learning from what has taken place in the recent period, and provides insights for acting carefully, preventively and in a future-proof manner in the near future. A book that takes its place in an interesting series of books from the editorial team.

Paul Baak and Wouter Bronsgeest
Co-chairs of the KNVI

Editorial

COVID-19 has the world in its clutches. Digitalisation can play an important role in combating the SARS-CoV-2 virus. One of the applications involves digital contact tracing in order to fight the spread of this infectious disease, a measure that dozens of countries have recently adopted. What is striking is that the events surrounding the contact-tracing apps ('COVID-19 apps') are accompanied by dilemmas and choices; they also sometimes provoke strong differences of opinion. About the social aspect, the technology itself and the legal framework. Controversies about these app-based tracing and warning systems for people who may be infected with the SARS-CoV-2 virus, ongoing new developments in this domain and national differences in the approach to and rollout of the project — considered individually or as a whole — constitute an interesting topic for research and can also serve as a point of departure for gaining insight into aspects of ICT and the digital society.

A number of these are considered in this collection, in addition to a few articles touching on other countries. Where do we stand, for instance, in terms of digital quality, including security aspects, architecture and technology, privacy protection in practice, European tendering, government ICT projects, the ethical side of digitalisation, the notion of open-source software, data-driven medicine, the costs of an automation project, cross-border data processing, the legal liability of software suppliers towards government organisations, attention for the supervision of ICT systems, and our independence from the US-based app stores?

The Royal Association of Information Professionals (KNVI) is ideally equipped to shed light on not only the social aspect but also the technology and the legal framework of the COVID-19 apps from a broader perspective. After all, the KNVI is *the* platform for digital and information professionals from various segments of society. We are particularly pleased that a few authors from the network of the International Federation for Information Processing (IFIP) also contributed to this new collection. The IFIP is the international federation of national associations for information processing, an NGO affiliated with UNESCO. Thanks go out to Leon Strous, former IFIP president, for his support in this endeavour.

It goes without saying that we also thank all the authors who contributed to this new collection. Together they made this book possible. The contributions were

expressly written in a personal capacity and were deliberately kept concise in nature. (In the event of multiple authors, the authors are listed alphabetically.) They contain valuable analyses and suggestions, but no advice for concrete cases. Above all, the texts unlock the insights and knowledge of today. The research for most of the chapters was concluded at the end of January 2021.

Natascha van Duuren, Victor de Pous Amsterdam, 10 March 2021

1 COVID-19 apps as survey point for ICT and the digital society

Victor de Pous

Digitalisation can play an important role in the fight against the SARS-CoV-2 coronavirus. Information systems collect tests, analyse data on spread, simulate infection risks or register vaccinations. Mobile applications with diverse objectives offer different functionalities, sometimes on the basis of artificial intelligence. At the same time, general information technology lends a helping hand. We work, operate and spend remotely *en masse*. From a legal perspective, the right to privacy carries a great deal of weight in healthcare. Europe has a stricter data-processing regime for special personal data, including information about our health, for instance. Especially in response to contact-tracing applications (COVID-19 apps) — for the purposes of an automated identification and warning system for people who may have been in contact with an infected person — dilemmas, choices and controversies arise each time; and not only in relation to the protection of our privacy. What do these events say about the different aspects of ICT and the digitalising society?

Widespread use

All sorts of ICT applications are being deployed in the fight against the infectious disease COVID-19.[1] In the Netherlands, the RIVM publishes a dashboard showing on the basis of updated figures how this coronavirus is spreading here.[2] One of the information suppliers is the Leiden University Medical Centre (LUMC). In order to get an accurate and up-to-date picture of how the virus is spreading, it launched COVID Radar at the beginning of April 2020.[3] The LUMC uses this app to collect data on both symptoms and people's behaviour. Researchers hope this can provide

[1] Also see: https://www.rijksoverheid.nl/onderwerpen/coronavirus-app/documenten/publicaties/2020/05/19/digitale-ondersteuning-covid-19.

[2] https://coronadashboard.rijksoverheid.nl/

[3] https://www.lumc.nl/over-het-lumc/nieuws/2020/April/covid-radar-app/

more insight into how the epidemic is unfolding, who is at greater risk, what impact social distancing has and where and when the need for healthcare may arise.

In contrast, the OLVG Corona Check app was developed for people with (mild) symptoms that may be caused by the coronavirus. From 16 March 2020 onwards, they have been able to use the Luscii app, operational since 2018, for COVID-19 self-management, guided remotely by the OLVG and consequently avoiding burdening the rest of the regular care system.[4] At that time, there was an enormous 'run' on healthcare capacity, and tests were not yet readily available. The system, now also being used by other hospitals and renamed Corona Check, uses artificial intelligence (AI).[5] The Maasstad Hospital also provides home monitoring, but then in relation to coronavirus patients who have been discharged from hospital.[6] Using this same Luscii app, these patients at home — those who are digitally literate — have, since July 2020, been forwarding measurement data on their blood oxygen saturation level, temperature and any symptoms and additional data to a medical team. Yet another application of AI. According to a trial by researchers from the Massachusetts Institute of Technology, an 'mHealth tool' can determine evidence of COVID-19 from a mobile telephone recording of a person's forced cough, even if the person is asymptomatic.[7] For the time being, the technology focuses on early, fast warning in the event of group diagnosis.

Yet another type of information system brings together certified medical screening data, such as negative tests and vaccination data. In October 2020, Cathay Pacific Airways and United Airlines started a trial with CommonPass, a mobile application that stores and verifies a passenger's COVID-19 test status.[8] This system checks whether the passenger satisfies the requirements of the destination country and generates a QR code. The aviation industry organisation is also working on this kind of digital 'health passport', the IATA Travel Pass.

The fact that besides dedicated healthcare-related ICT, other types of systems can be worthwhile is evident from the *en masse* shift of activities to online,

---

[4] https://www.olvg.nl/nieuws/olvg-corona-check. This functionality was developed over two days. https://www.olvg.nl/nieuws/olvg-corona-check-meer-informatie-voor-huisartsen

[5] For a broad discussion of this topic, see Natascha van Duuren, Victor de Pous (eds.), *Multidisciplinaire aspecten van artificial intelligence [Multidisciplinary aspects of artificial intelligence]*, Amsterdam, 2020.

[6] https://www.maasstadziekenhuis.nl/specialismen-afdelingen/longgeneeskunde/meer-weten/thuismonitoring-corona-covid-19/

[7] The publication is from 29 September 2020. https://ieeexplore.ieee.org/document/9208795

[8] https://commonpass.org/

including working from home and online shopping. But there is more. Pseudonymised traffic and location data from mobile phones offer the possibility of monitoring congestion and movements on the level of the population. It is generally assumed that the information helps in detecting new resurgences of the virus early on by counting people. This information derived from telecom data is being used in efforts to combat the virus in many EU countries, with the exception of Malta and the Netherlands. Aside from the question of whether a law is necessary for this, the Lower House is wrestling with the proposal submitted on 29 May 2020 for the Temporary Act RIVM Information Provision in connection with COVID-19 that would make this modus operandi possible in the Netherlands.[9] A sense of urgency is evidently lacking.

SARS and Ebola

Without a vaccine or medication for a contagious disease, quarantine, source and contact investigation and social distancing are the most important measures for preventing the spread. The concept of algorithmic or automated contact tracing, particularly via mobile technology, has been around since at least 2007, in relation to SARS.[10] As far as is known — and most likely independent of this — Germany was a frontrunner in practice, but in relation to the Ebola epidemic that hit West Africa in 2014.[11] Implementation did not occur quickly. Cooperating ICT companies from Leipzig, Chemnitz and Dresden worked for five years on building a GPS and Bluetooth-based contact-tracing app.[12] It was a private, philanthropic project. What is striking is that the infectious diseases specialist involved, Thomas Grünewald, said on 30 October 2019: "Wenn die App funktioniert, wäre sie eine Vorlage für andere Infektionskrankheiten, die wie Ebola viele Menschen in kurzer Zeit betreffen können." He was thinking of a flu (influenza), SARS and measles; and not just in Africa.[13]

[9] https://www.rijksoverheid.nl/documenten/kamerstukken/2020/05/29/wetsvoorstel-telecommunicatiewet

[10] http://www.inderscience.com/offer.php?id=13540

[11] https://www.tagesspiegel.de/wissen/warnung-per-push-nachricht-wie-eine-smartphone-app-aus-deutschland-vor-ebola-schuetzen-soll/25167852.html

[12] https://www.sachsen-fernsehen.de/tag/alexander-stinka/#

[13] https://www.tagesspiegel.de/wissen/warnung-per-push-nachricht-wie-eine-smartphone-app-aus-deutschland-vor-ebola-schuetzen-soll/25167852.html

The idea for the app came from the honorary consul of the Republic of Liberia in Germany, Michael Kölsch, who was confronted at that time with the dramatic effects of the Ebola virus. Because virtually everyone in Africa has a mobile telephone, the technology might help to warn people early on about contact with an infected person. That proved to be correct.

New coronavirus

In relation to COVID-19, more than 50 countries now use both manual contact tracing via interviews and questionnaires and automated contact tracing. This kind of ICT system for the process of identifying and warning people ('contacts') who may have been in contact with an infected person is, as a rule, supported by a mobile application: a COVID-19 app.

In the Netherlands, the combined discussion on this, i.e. in factual and legal terms, began after the cabinet's emergency meeting on 7 April 2020 when Minister De Jonge (Public Health, Sport and Welfare) — following suit from countries such as South Korea (app available: 11 February 2020) and Singapore (20 March 2020) — announced that the government was considering the use of apps, two even, in combating COVID-19. "One that notifies you if you have been in the vicinity of another user who has emerged to be infected, in which case you are advised to stay indoors and asked to use a second app that enables you to easily stay in contact with a local doctor."[14]

Dilemmas, choices and controversies

You see it everywhere. Digital contact tracing for the purpose of combating this infectious disease goes hand in hand with dilemmas and choices and sometimes provokes strong differences of opinion, especially in the western world. About the social aspect, the technology itself and the legal framework. To get development off to a flying start, the Ministry of Public Health came up with an 'appathon'.[15] The attempt at a quick, creative development process failed. The public tendering procedure fell short, and the quality of the proposals was substandard. In fact, the multiple deficiencies even prompted 50+ organisations and individuals to draft a

[14] https://www.rijksoverheid.nl/documenten/mediateksten/2020/04/07/letterlijke-tekst-persconferentie-minister-president-rutte-en-minister-de-jonge-na-afloop-van-crisisberaad-kabinet

[15] See chapter 5 for more on this appathon.

manifesto outlining ten starting points that an app must comply with.[16] The input from the ad hoc coalition *Veilig tegen Corona* [Safe against Corona] subsequently functioned as informal citizen participation in a national government automation project. Probably the first of its kind; also because the ministry had hired a number of criticasters.

Despite the dozens of countries that have their own COVID-19 app operational, opinions are still divided on the usefulness or necessity of these. Also taken into account is the fact that the effectiveness of the application depends on a number of factors, such as the percentage of active users in an area, the possibility of getting tested (quickly) and, of course, the willingness to report infection.[17] More is needed, therefore, than just a well-designed, technically secure app (and back-end server) incorporating privacy by design.

The issue of privacy, other fundamental rights and the democratic rule of law quickly arose. The Electronic Frontier Foundation often fulfils a guiding role, even outside the US. The US foundation sounded the alarm on 3 April 2020. To summarise, surveillance via apps "invades privacy, deters free speech, and unfairly burdens vulnerable groups".[18] This was followed one week later by another statement on principle: "Contact-tracing applications cannot make up for shortages of effective treatment, personal protective equipment, and rapid testing, among other challenges."[19] Or, to cite the American Civil Liberties Union (ACLU), these digital resources (the apps) "are unlikely to work, and that the debate over such tracking is largely a sideshow to the principal coronavirus health needs".[20]

CoronaMelder

In the Netherlands, too, among other things the fundamental precondition that the app can actually help combat the virus has led to division. Of the 50 signatories of the above-mentioned manifesto, at least four — Bits of Freedom, Waag, Amnesty International and Platform Burgerrechten — felt that the current CoronaMelder

[16] https://www.veiligtegencorona.nl/. The German Chaos Computer Club was ahead of them https://www.ccc.de/de/updates/2020/contact-tracing-requirements

[17] For more on this, see chapter 2.

[18] https://www.eff.org/deeplinks/2020/04/how-eff-evaluates-government-demands-new-surveillance-powers

[19] https://www.eff.org/deeplinks/2020/04/challenge-proximity-apps-covid-19-contact-tracing

[20] https://www.aclu.org/news/privacy-technology/tracking-apps-are-unlikely-to-help-stop-covid-19/

('Corona Notifier') app did not adequately satisfy the defined criteria.[21] In summary, the app reportedly 'did not bridge the gap' between technology and society, for example because it did not provide the possibility of immediate testing after notification. Incidentally, with effect from 1 December 2020 it became possible to get tested even without symptoms; and indeed from day five onwards.

Medical professionals take a different view of such applications. A more pragmatic view could be heard from Niels Chavannes, professor of e-health at the LUMC. "The app was initially presented as a wonder drug. That is not the case, of course. But every little bit helps."[22] For the record, the CoronaMelder app is the result of an entirely new development process, which moreover became publicly available under an open-source licence from the start. Third parties — individual citizens — can assess the software code and themselves submit suggestions for improvement. That has happened.

Opinions also remain divided on the need for a special law for the Dutch COVID-19 app, although such a basis now exists, contained in section 6d of the Public Health Act. From the viewpoint of privacy protection, the Dutch Data Protection Authority (Dutch DPA) considers a statutory regulation the appropriate basis for the processing of personal data. Minister De Jonge and the State Advocate take the view that consent from the data subject suffices as a valid ground for data processing via the mobile application. Nonetheless, the regulation was introduced. The Temporary Act on the COVID-19 Notification Application took effect for a three-month period on 10 October 2020 and was extended to 21 April 2021.[23]

Umbrella organisation GGD GHOR Nederland and the Ministry of Public Health then together started using a second app, GGD Contact. This application makes it possible to notify contacts about an infection faster; it therefore also supports source and contact investigation.[24] On 20 November 2020, the engineering association KIVI reported that a third coronavirus-related government app could still be introduced, CoronaTester, for efficient access to various tests, while the software could also serve as proof of a negative test result.[25] In the letter

[21] https://www.veiligtegencorona.nl/analyse.html

[22] https://nos.nl/artikel/2351218-kan-de-corona-app-helpen-deze-deskundigen-denken-van-wel.html. In particular, see chapter 2 of this collection.

[23] https://wetten.overheid.nl/BWBR0044194/2020-10-10

[24] https://ggdcontact.nl/ The first practical tests were started in West-Brabant in mid-December 2020, in Rotterdam-Rijnmond at the beginning of January 2021 and subsequently in Twente.

[25] https://kivi-corona.blogspot.com/2020/11/coronatester-app-help-met-je-ict-team.html

to the Lower House of 23 February 2021, Minister De Jonge talked about the CoronaCheck app as digital proof, while, for the record, an alternative would also be introduced for people without a mobile phone.[26] On closer inspection, it concerned the CoronaTester, the name of which had changed; also from GGD GHOR.

In conclusion

Controversies about app-based tracing and warning systems for people who may be infected with the SARS-CoV-2 virus, ongoing new developments in this domain and national differences in the approach to and rollout of the project — considered individually or as a whole — constitute an interesting topic for research and can also serve as a point of departure for gaining insight into aspects of ICT and the digital society. A number of these are considered in this collection, in addition to a few articles touching on other countries. Where do we stand, for instance, in terms of digital quality, including security aspects, architecture and technology, privacy protection in practice, European tendering, government ICT projects, the ethical side of digitalisation, the notion of open-source software, data-driven medicine, the costs of an automation project, cross-border data processing, the legal liability of software suppliers towards government organisations, attention for the supervision of ICT systems, and our independence from the US-based app stores?

A few general analyses

- German ICT companies were front-runners with a contact-tracing app, probably worldwide, in response to the Ebola epidemic in West Africa in 2014. Ebolapp became available in test form at the end of 2019.[27] Only the physician can read out data from the app, while the data are registered in encrypted format locally on the telephone and are processed in accordance with German law for health data.[28] While version 2.0 was also suitable for COVID-19 from the beginning of March 2020, it appears that the application remained almost entirely under the radar.

[26] Letter on COVID-19 state of affairs and cabinet response to the 100th and 101st OMT recommendation,
https://www.tweedekamer.nl/kamerstukken/brieven_regering/detail?id=2021Z03637&did=2021D08036

[27] https://www.ebolapp.org/

[28] The back-end server is in the Federal Republic. https://www.ebolapp.org/#daten

- "The current coronavirus crisis demonstrates once again: digital infrastructure is indispensable. The medical care to which the Netherlands owes so much gratitude over these months cannot function without stable and flawlessly functioning communication and ICT networks", the telecommunications supervisory authority Agentschap Telecom said on 27 August 2020.[29] The applications function somewhat less flawlessly. The daily hospital admission figures are sometimes delayed, the Infectieradar (Infection radar)web tool (from RIVM) contains a serious data leak, and the vaccination programme encountered delays in part because an information system was not in order. And, at the beginning of February 2021, after six months of availability, the Coronatest.nl website still did not comply with six of the security standards for the use of DigiD. CoronaMelder stands out well, but this was unable to prevent significant data leaks at GGDs and at a commercial testing company.

- Health communication is considered so important in the Netherlands that the University of Amsterdam has appointed chairs in this area. In mid-January 2021, professors Bas van den Putte and Julia van Weert described the government's communication policy in combating the pandemic as a failure.[30] We notice that the various coronavirus-related apps can cause confusion among citizens. These are applications (i) with divergent functionalities, (ii) from private or government organisations and (iii) many — but not all — of which contain 'COVID' or 'Corona' in their name, with some apps changing their names at times. For instance, CoronaTester from the GGD GHOR suddenly became CoronaCheck; the same name as the app used by hospitals for patient self-management, with distance care.

- Despite the strict regime under the General Data Protection Regulation (GDPR), the restrictive interpretation of the law by the Dutch DPA, and a ban on discrimination in the use of the CoronaMelder app in the Temporary Act Notification Application COVID-19, the important starting points that consent for the processing of health data must be given 'freely' and 'voluntarily' with regard to the use of apps are under pressure. That applies for the citizen as

[29] https://www.agentschaptelecom.nl/actueel/nieuws/2020/08/27/de-digitale-transitie-scenario%E2%80%99s-kansen-kwetsbaarheden-en-toezicht

[30] Het Parool, 19 January 2021.

employee and, for example, as consumer. Certified screening data (negative test results, and now also vaccination information) will most likely be increasingly desired, whereby apps — like a digital health passport[31] — support the provision of evidence; also because according to the latest insights, COVID-19 is expected to become endemic.[32] No QR code, then no access or use of a service.

[31] There will probably (also) be an EU vaccination passport.
https://www.consilium.europa.eu/nl/press/press-releases/2021/02/25/statement-of-the-members-of-the-european-council-on-covid-19-and-health-25-february-2021/

[32] https://nos.nl/artikel/2370489-wetenschappers-coronavirus-gaat-niet-meer-weg.html

2 The use(lessness) of contact-tracing apps

Gabriëlle Speijer

We write during the first week of April 2020, in the midst of the first wave of the coronavirus pandemic. The Netherlands is in an 'intelligent' lockdown. Out of the blue, the Ministry of Public Health, Welfare and Sport announced an 'appathon' for the purpose of selecting two types of apps: one aimed at monitoring the development of COVID-19, the other at warning citizens. One day in advance, the plans changed, for reasons unknown, whereby the process became strictly focused on the development of a contact-tracing app. The objective was to introduce this in the shortest timeframe possible in order to get our country out of lockdown, whereby the mobile applications were to serve as the core for the testing policy in the future. More than six months after having jointly written to the ministry during that now notorious Easter weekend — also in view of the many questions about the how and why — we analyse the use and uselessness of such automated systems in combating the pandemic. Where do we stand now?

No one is safe if not everyone is safe

COVID-19 is caused by the SARS-CoV-2 virus that spreads between people via droplets and contact transmission. In order to control the spread of COVID-19 — in the absence of immunity/an effective vaccine — interventions are needed to break the transmission chain so that the R number (effective reproduction number) remains less than 1. As part of an all-encompassing strategy, identification, isolation, testing and provision of cases, contact tracing and quarantine are among the actions critical to reduce transmission.[33]

With the 'Test and Trace' pilot, Kendall et al. demonstrated that this strategy resulted in a smooth decrease in secondary infections — also for COVID-19 — and as such, a curtailment of the scope of the first wave of the pandemic.[34] These kinds

[33] https://www.who.int/publications/i/item/contact-tracing-in-the-context-of-covid-19

[34] Lancet Dig://it Health 2020; 2: e658-66

of trial projects cannot be unreservedly translated to a different location, however. This is because the success of test and trace is influenced by a variety of factors, such as social involvement and culture, training and availability of personnel, logistical support *and* the availability of real-time data with expertise on hand for interpretation and reporting.

Pandemic preparedness

The speed of intervention is crucial,[353] as also emerged in practice. For instance, in Taiwan[36] — supported by trained personnel and with the outbreak of SARS-CoV in 2003 still fresh in the collective memory[37] — every newly diagnosed case was rapidly isolated.

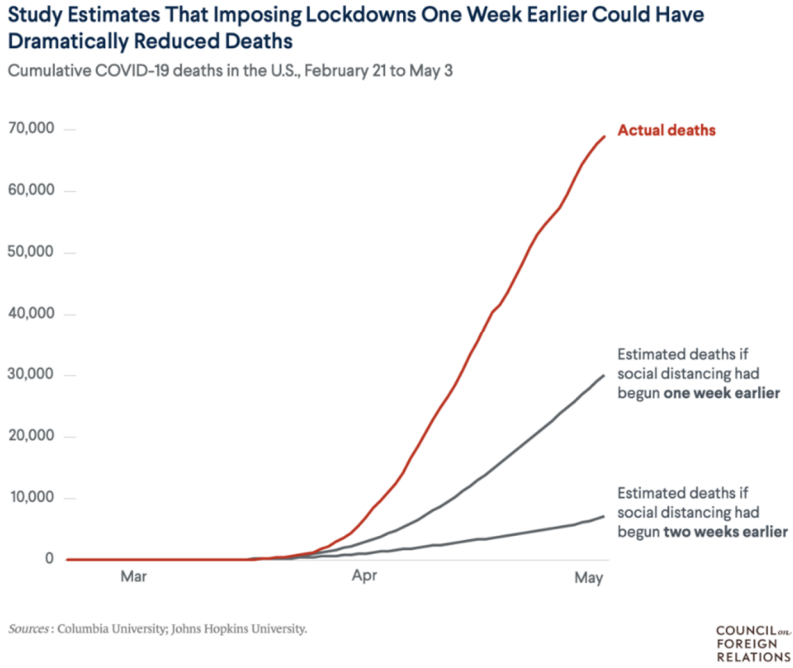
And yet we also saw countries outside of Asia that managed to smoothly get the virus under control. The MERS-CoV epidemic helped Saudi Arabia with a more alert public health system, infection control policy and measures (a number of extreme interventions were already taken in mobility, social and religious gatherings, travel and business even before the country's first COVID-19 case).[38] But also Senegal, where experience with Ebola had resulted in a blueprint for combating disease via mobile testing locations and also widespread public trust in the government. Translating scientific and public health expertise into administrative policy quickly and clearly proved crucial. Considerations at the expense of combating the virus cost dearly: in victim numbers, more serious economic damage as a result of lockdown, and a decline in public trust in policymakers.

[35] https://tfr-2020.cfr.org/report/pandemic-preparedness-lessons-COVID-19/findings/#tfr2020_what_went_wrong_domestically

[36] JAMA. 2020;323(14):1341-1342

[37] J Autoimmun. 2020 Jul;111:102487

[38] https://pubmed.ncbi.nlm.nih.gov/32451260/



How do we place the gains?

Apps — mobile applications — could be seen as part of the larger whole of (digital) tracing, but the functionality and underlying technology does differ. This can include GPS tracking, mobile telephone data, Bluetooth, combination with other applications such as credit card data, selfies at locations. The objective of a contact-tracing app is to (help) reduce the R number so that outbreaks can be prevented, while simultaneously limiting the number of people in quarantine.

Reducing the time between isolation of the case (including pre-symptomatic contagious phase) and quarantine of the contact people by gains in tracing speed is the added value of a contact-tracing app.[39] It can also serve as a supplement to the reach of the traditional (human form of) contact investigation, because even people who are not acquaintances of an infected person can be detected. In this way, the app is seen as a solution for lifting and preventing lockdown, in order to

[39] https://science.sciencemag.org/content/368/6491/eabb6936

allow social life to resume (in part), with the reopening of public transport and public spaces, for instance.

More fine-tuning of policy could also be possible through targeted insight on the local level, perhaps to be considered a form of precision epidemiology. This could then be generated by combining these app data with, for instance, data on changes in symptomatology, behaviour and other factors. Other advantages of digital contact tracing are, among other things, the low costs and its scalability, and the added value as assistance in guiding the deployment of costly resources to combat the virus.

Models

Simulations by Hinch et al. assume that 80% repression of epidemic is possible if 56% of the population is willing to participate in app-based tracing.[40] In an ideal setting (see infrastructure considerations), this should result in 36% of infections being identified. The percentage based on the voluntary download of the CoronaMelder app was at just over 4.36 million downloads as of 29 December 2020. Approximately 25% of 17.5 million residents, this amounts to approximately an extra 6% of infections being identified with the help of digital tracing under the ideal conditions.[41] This number corresponds to the yield, based on the data available to date, from which around 4% of positive tests were traced with the CoronaMelder app among asymptomatic people.

In November 2020, the same group published in cooperation with Google Research, based on a model representative for the state of Washington, that 15% app use would result in 15% COVID-19 infection reduction if combined with the traditional tracing (in the most optimal utilisation) and in 8% infection reduction in the event of only digital tracing.[42]

[40] https://cdn.theconversation.com/static_files/files/1009/Report_-_Effective_App_Configurations.pdf?1587531217

[41] https://cdn.theconversation.com/static_files/files/1009/Report_-_Effective_App_Configurations.pdf?1587531217

[42] https://www.medrxiv.org/content/10.1101/2020.08.29.20184135v1.full.pdf

Based on Dignum et al., it emerged on the basis of unique simulations that included both an epidemiological model and behavioural effects that an app in a situation of even 60% adoption made no significant contribution to combating the virus.[43]

Not a stand-alone intervention

With all efforts to develop a reliable, well-functioning and secure system for digital tracing in the event of a pandemic, we must realise that the technology must be embedded throughout the testing and tracing system. The following matters must also be taken into account:

1. **App reliability related to:**
    I. 'Testing': proportion of people who test positive who are also reported via the app, the availability of testing at a reasonable distance, time between test and result, infection rate among the population (the higher the rate, the less reliable).
    II. Functionality: how reliably are contacts identified using the app? How seriously do people follow the instructions?
2. **Adoption rate in the population (number of downloads and actual use).**
3. **Performance of the underlying technology, including:**
    I. *Overwhelming* in the event of false alarms
    II. Privacy concerns
    III. Communication (broader than substantive, including things such as user experience, personalised notification, ongoing analysis for improvement and the use of specialised human interaction) of reports via the app

    Secondary to underperformance, behavioural change is another lurking factor. Which results not only in reduced adoption of the technology, but also a decrease in compliance with measures to combat the virus.
4. **More widespread embedding in traditional contact tracing and government advice.** A limited understanding of government measures in relation to lockdown and the corresponding effects on the decrease in COVID-19 emerged to be associated with limited willingness to participate in

[43] https://simassocc.org/assocc-agent-based-social-simulation-of-the-coronavirus-crisis/news-and-publications/

app-based contact tracing.[44] Other factors include to what extent and how guidance by the specialised team is provided via the app, whether people can contact someone if they have questions, how this is responded to, whether account is taken of and assistance provided in relation to quarantine advice, such as finding accommodation, arranging aftercare, and so forth.

5. **Cultural embedding, public expectations and perception of digital tracing.** A contact-tracing app could have more impact in a more totalitarian regime than the Netherlands, where it is voluntary. Is compliance on the part of the population affected by rapidly changing measures in relation to social distancing, the indirect effects of economic disruption or mental health deterioration and other indirect health consequences such as the deferment of oncological care?[45]
6. **Potential long-term effects of the digital tracing technology** in society. A collaboration between Google and Apple in relation to Bluetooth technology, as used for the CoronaMelder app, could be conducive for numerous other solutions — desirable or otherwise — at a later stage.[46]

Scientific validation?

The importance of, from the terms of reference onwards, including every multidisciplinary perspective (ethical, political, legal, technical, behavioural, sociological, philosophical, etc) on which digital tracing technology is crucial since introduction is not a neutral or non-committal intervention. After all, it may even result in (permanently) harmful consequences, including false security, with reduced control as a result, and behavioural change with even deferred effects on society.

How models relate to reality and the constantly changing underlying factors therein, such as the effect on behaviour of a package of measures, whether or not rapidly changing, as part of government policy, deserves attention for everyone in the society. Especially in the light of the dashboard rage as a by-product of the crisis. Besides awareness of the complexity of reality compared to the simplified representation in a model, scientific validation is required; preferably in randomised research.

[44] https://simassocc.org/assocc-agent-based-social-simulation-of-the-coronavirus-crisis/news-and-publications/

[45] https://pubmed.ncbi.nlm.nih.gov/32702310/

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

Conclusions

Without pharmaceutical intervention, the success of combating infection lies mainly in a rapid and resolute response from the healthcare authorities and implementing supervisory services with a focused testing strategy. The contribution of digital tracing can be one component of that, but decidedly not one that is separate from the overall system of measures and factors. Based upon a few practical figures from the past months and epidemiological models, the CoronaMelder and similar apps make at best a very limited contribution, with a percentage of between 4 and 8% in terms of extra infections traced.

Even though this percentage is low, it could indeed be a supplement to the traditional testing and tracing, because this method enables the tracing of persons who may potentially become infected (for example in public transport) without being someone the COVID-19-positive person knows. Traditional contact tracing, which assumes specific knowledge and skill, is in the foreground. The personal approach is crucial to ensure that measures are and can be complied with. Based on the presumption that the population takes responsibility for health (their own health and that of others), an app can also yield time gains (by omitting the intermediary, such as a GGD).

In conclusion, the use or uselessness of an app such as the CoronaMelder, whereby privacy is safeguarded so that there is no automatic insight from the traditional test and trace system, depends entirely on the behaviour of the population. As such, the contribution of the app depends on various culturally related aspects, which was confirmed in the studies over the past year.

Because technology is anything but neutral in use and deployment, it is essential to also anticipate the least optimistic flip-side. Here one could consider, for instance, the possibility that a technical solution specially developed for this purpose might be used for other purposes, or that individuals may see use of the app as a sort of licence for less strict compliance with behavioural recommendations, born from a false sense of security.

Assessing the contribution of measures in combating the virus is extremely complex, since effects can also change over time. There is currently no scientific validation in randomised research of an app's contribution, and it is therefore questionable whether this might not also be too complex and costly. What the app without any scientific evidence has indeed brought about is a discussion about fundamental values in our society, about how we relate to technology and our fellow man. Awareness needs to be raised in relation to the fact that technology is

not a 'no strings attached' instrument. This applies for the use of technology, but also for coordination ahead of any implementation. Constant steering based on our fundamental human values, based on a multidisciplinary approach, is crucial.

Analyses

- An app as a stand-alone solution can, with reference to the analysis above, be placed in the category of *tech solutionism* or, as the case may be, useless. Focusing on an app that protects privacy, with the inclusion of multidisciplinary experts later in the process, is an undesirable situation because of the diversity of factors that influence the overall process of combating the virus, but also in particular related to the app. In this last case, it involves, for instance, cyber-physical interaction and the behavioural effects related to this.

- From the formulation of the terms of reference through to selection, continued development and possible replacement of an app as part of digital tracing, the starting point must be that multidisciplinary expertise must be represented with a transparent contribution, supported on a scientific basis, with an eye for any pitfalls or concerns that must be taken into account.

- Such an innocent app — even based on an open process — can cause effects that can manifest much more broadly in society. With all the implications this has for combating the virus, but also for numerous other domains in our society.

- Early acknowledgement or recognition of a crisis, daily public briefings and simple unequivocal messages in relation to health, and a transparent and respectful attitude towards scientific and medical/public health expertise on the part of policymakers deserve explicit attention. With a side note that for the last groups mentioned, training and guidance in (social media) communication could still use a significant boost for the benefit of public trust.

3 A different kind of antivirus: the technology and data logistics of contact-tracing apps

Marco Bommeljé

As COVID-19 claims human lives all over the world, many tens of millions of people have become infected and healthcare workers are working overtime to save lives, it seems frivolous to be devoting attention to the development of contact-tracing apps (COVID-19 apps). And yet it is important to pay attention to this, because some technical aspects of these mobile applications and their underlying systems, such as the detection of high-risk contacts and data storage models, have major impact. The way in which the various apps have been created and the architecture choices made in this process can teach us important lessons. Lessons for after this pandemic, when people continue shaping the digital world. With growing digitalisation, it is becoming increasingly important that the people designing and building systems take into account the impact that technical choices have on the quality of society.

Source and contact investigation

Like many other contact-tracing apps, the Dutch CoronaMelder app was developed to support source and contact investigation in relation to people who have become infected with the coronavirus.[47] Traditionally this investigation takes place in the form of interviews, but the modern smartphone has a technological range that one assumes can help track down high-risk contacts. After all, smartphones are able to determine their geographic location relatively accurately and can pick up on other

[47] Coronavirus-related apps can be categorised according to their main purpose. Many have the aim of tracing contacts who are at risk of infection. Others primarily serve to inform the user about the current situation in their environment. And yet other apps are intended to recognise symptoms and use symptoms questionnaires for the user to fill in. The apps for information provision and symptom registration, such as CovidRadar from the RIVM, have been left out of consideration here.

smartphones in the immediate vicinity. Location determination uses the presence of radio signals (GSM, GPS, Wi-Fi). Smartphones recognise other smartphones in their vicinity via Bluetooth, usually Bluetooth Low Energy (BLE).[48]

So it was no surprise that when the pandemic broke out around the world, there was a call for smartphones and other ICT to be used in combating it. China and Singapore were among the first countries where these were actually used to contain the spread of the virus[49], but in the course of March and April 2020, more app projects arose, in Europe as well, including the Netherlands.[50]

Positioning and determining distance

Despite all the optimism and decisiveness, it was unclear how effective the smartphone technologies would be for detecting contacts at risk of infection. The positioning technology used by smartphones is based on radio signals from GSM antennae, GPS satellites[51] and Wi-Fi internet access points (hotspots) with a fixed location. Triangulation measurements by GSM antenna signals are accurate to within about 20 metres. GPS is more accurate and provides a radius of 5 metres. Wi-Fi signals have a reach of at most a few dozen metres and can be used for positioning if the transmitter's location is known. Modern smartphones combine the different radio signals, but the accuracy is still about two metres at best, but in practice three to seven metres.[52]

Smartphones recognise other smartphones in their vicinity and estimate distance via Bluetooth, usually Bluetooth Low Energy (BLE).[53] A BLE signal can reach

[48] See, for instance: https://tweakers.net/nieuws/166380.html, https://medium.com/personaldata-io/-fe7badc2bb6d en https://pact.mit.edu/wp-content/uploads/2020/11/SonicPACT_Final_v2-with-logos-revA.pdf

[49] The BBC first reported on the Chinese app on 11 February 2020. In Singapore, TraceTogether was published on 20 March 2020 (https://www.bbc.com/news/technology-51439401).

[50] For an overview of frameworks for digital contact tracing, see: Tania Martin, Georgios Karopoulos, José L. Hernández-Ramos, Georgios Kambourakis, Igor Nai Fovino, 'Demystifying COVID-19 Digital Contact Tracing: A Survey on Frameworks and Mobile Apps', Wireless Communications and Mobile Computing, vol. 2020, Article ID 8851429, 29 pages, 2020. https://doi.org/10.1155/2020/8851429

[51] See, for instance: https://en.wikipedia.org, https://www.gps.gov/systems/gps/performance/accuracy/ and (http://unwiredlabs.com/coverage.

[52] Smartphone GPS accuracy may affect contact-tracing (https://news.uga.edu/smartphone-gps-accuracy-affect-contact-tracing/)

[53] See, for instance: https://tweakers.net/nieuws/166380.html.

to about 70 metres in a direction without obstacles. This technology was originally introduced by Nokia in 2006 for applications in which a transmitter sends out signals to all recipients within reach. With Apple's introduction of BLE beacons from 2013 onwards, this technology became a building block for what is referred to as the Internet of Things (IoT), which was a new hype a few years ago but which has since become an invisible part of the digital surveillance arsenal. Estimating distances between smartphones on the basis of signal strength is inaccurate, however, because the signal is heavily influenced by the environment. Some researchers therefore propose using ultrasonic sound in supplement to BLE.[54]

The technologies for both positioning and proximity detection lack the accuracy that is actually required and fortunately do not yet see everything.[55] Irrespective of which technology is used, recognising contacts at risk of infection remains a difficult issue. Most COVID-19 apps in Europe now use the BLE technology to trace smartphones in the immediate vicinity.[56]

Proximity tracing

A COVID-19 app that supports source and contact investigation registers what other smartphones are in the vicinity and for how long. This is called 'proximity tracing'. How does it work? The COVID-19 app periodically sends out a signal and registers the signals from other smartphones on which the app is active. The signal contains little more than the identification of a sender.[57] The app then keeps a log of contacts, recording for each contact the estimated distance, time duration and of course identification. Some countries have a COVID-19 app that also keeps track

[54] https://pact.mit.edu/wp-content/uploads/2020/11/SonicPACT_Final_v2-with-logos-revA.pdf

[55] Smartphones that are laid on a table while the owners are sitting adequately distanced, or the smartphones of school pupils that have been collected by the teacher during a test.

[56] Apple and Google have prohibited the use of positioning for COVID-19 apps that use the Bluetooth Low Energy API developed by them and known as GAEN (Google Apple Exposure Notification). So there is little left to choose from.

Reuters. Apple, Google ban use of location tracking in contact-tracing apps (4 May 2020). https://www.reuters.com/article/us-health-coronavirus-usa-apps-idUSKBN22G28W

[57] In the BLE technology developed by Apple and Google that is now being used for contact tracing, the payload of the signal consists of, in addition to the identification, an indication of the signal strength and the type of transmitting smartphone. https://covid19.apple.com/contacttracing

of location.[58] If someone is diagnosed as a coronavirus carrier, their contacts can be found in the log and the persons at risk of infection can be warned. Although the information recorded appears minimal, it does involve data that can be traced back to people: personal data, therefore.

As soon as it became clear that large-scale digital contact tracing would play a role in combating the spread of the virus, concerns were voiced from all sides about privacy and data protection.

Are the measures as strict as they sound?

'Better to blow on the soup than burn your mouth' is the motto when soup is served. That applies in this case as well. When all contact data are recorded in their original state, a person's private life can be made visible in detail and searchable:

- all meetings (*the interaction graph*);
- the social network (*the social graph*);
- places where the person stays and their movements (*location traceability*), if the app registers location.[59]

The registration of contact data could therefore constitute a significant breach of the fundamental right of privacy, while users only need to know whether they are at risk of infection. They do not need to know *who* the high-risk contact was, or *when* or *where* that occurred. The same applies for the organisation carrying out the source and contact investigation. In fact, that organisation only needs to know that a tested person is infected, if the app itself can send the warning notifications.

An individual person who has tested positive can approve access to the data on his smartphone for the purposes of source and contact investigation, but that string of contact data also contains the personal data of other app users. And if the data of *all* users were to be stored centrally, everyone's privacy would be in jeopardy.

The biggest risk here is 'mission creep', whereby an information system acquires a different, less innocent, application over time. History shows that this is a real threat. The category 'religion' in the population records is the tragic example

[58] The coronavirus apps of various countries keep track of geographic location. Registering locations could be a possibility for detecting places with a high number of infections. See also note 17.

[59] MIT Technology Review keeps a database of characteristics of the coronavirus apps in 49 different countries. In sixteen countries, the coronavirus apps explicitly keep track of geolocation. https://www.technologyreview.com/2020/05/07/1000961/launching-mittr-covid-tracing-tracker/

from World War II. The reminder of this prompted protest when the 'Sofi' number was introduced in 1989. Despite promises from the government, it has gradually devolved into a personal 'citizen service number', which makes the linked government administration systems a panopticon for permanent surveillance of citizens.[60]

That means that the way in which COVID-19 apps store data is not just a technical design decision, but a decision with potentially far-reaching implications. Fortunately most designers of the COVID-19 apps have thought about this. An important first step is to periodically change the smartphone identification and encrypt it each time. In that case, the data that the app receives and registers cannot be automatically linked to a smartphone and therefore to a person. The degree of protection that this encryption provides does depend on the data logistics, i.e. the way in which the app and the underlying system deal with the storage and distribution of data and encryption keys.[61]

The centralised model

COVID-19 apps generally involve two models of data storage and processing, centralised and decentralised. TraceTogether (Singapore) and TousAntiCovid

[60] Wieringa, Tommy (10 April 2015) Niemands meester, niemands knecht [No one's master, no one's slave]. Kousbroeklezing 2015, and Het Inlichtingenbureau. Ze weten alles van je [The Intelligence Agency: they know everything about you]. (2021, 27 January). De Groene Amsterdammer, 2021(4). https://groene.nl

[61] Where the measures are indeed as strict as announced is the People's Republic of China. Privacy was certainly considered there. Privacy is suspect, it seems. China is fighting the pandemic with the use of the full digital surveillance arsenal, not only with location data from smartphones and mandatory check-in points, but also with 200 million cameras in public spaces, which are equipped with instantaneous (real-time) facial recognition. The use of the coronavirus app is compulsory. The app assigns users colour codes (red, yellow, green) that stipulate where someone may or may not be. Not much is known about the functioning of the app, but what is certain is that the location and movements of all Chinese residents are being tracked. China Mobile, the telephone company, published an app that can reconstruct the movements of every passenger in the past thirty days. Systems were also installed in public transport that can observe the health of travellers. A Big Data nightmare.
https://www.nytimes.com/2020/03/01/business/china-coronavirus-surveillance.html
http://www.xinhuanet.com/english/2020-02/10/c_138770630.htm
https://www.eni.com/en-IT/digital-transformation/china-fights-coronavirus-with-apps.html

(France) use the centralised model. That largely works as follows.[62] A user registers with the central system (back-end). The smartphone receives a series of encrypted codes, each of which constitutes the smartphone identification for a limited time. This means that only the central system can identify a smartphone on the basis of the encrypted codes. The coronavirus app therefore only receives coded smartphone identifications from other smartphones.

If someone tests positive, he or she contacts the health service, which issues an authorisation code enabling him or her to deposit the data collected by the app in the central database. The central system searches which contacts are at risk of infection and then deciphers the codes in order to provide the user records with a risk status. The app regularly checks the risk status in the central system and can thus warn the user.[63]

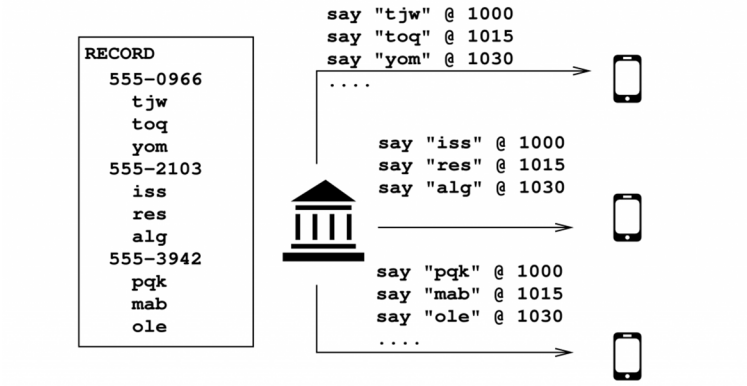


Figure 1. Centralised model: allocation of encrypted identities that change every fifteen minutes[64]

[62] TousAntiCovid is based on the ROBERT protocol, which is an elaboration of the PE-P3T specification, the Pan European Privacy Protecting Proximity Tracing, a collaboration between INRIA and Fraunhofer. https://github.com/ROBERT-proximity-tracing/documents and https://github.com/pepp-pt TraceTogether uses the so-called BlueTrace protocol. As of a few months ago, the app is equipped with SafeEntry, a digital access pass for certain public buildings. SafeEntry is increasingly required, so that since December 2020, TraceTogether is being used by more than 60% of Singapore residents. https://www.tracetogether.gov.sg/ https://www.developer.tech.gov.sg/technologies/digital-solutions-to-address-covid-19/tracetogether

[63] The manner of working described applies for TousAntiCovid, cf. DP3T White Paper p.44.

[64] The figures have been taken from https://blog.appcensus.io/2020/12/04/proximity-tracing-in-an-ecosystem-of-surveillance-capitalism/

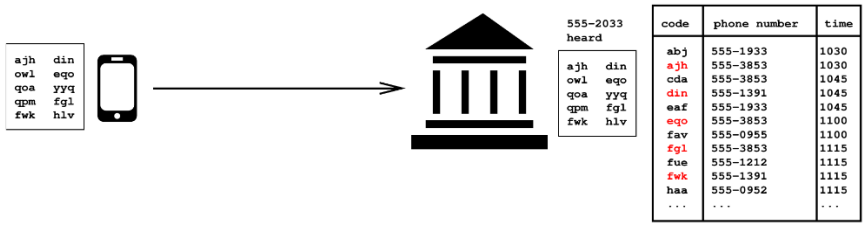


Figure 2. Centralised model: person who has tested positive submits contact data centrally and the authority selects people at risk of infection.

The centralised model clearly falls short when it comes to protecting privacy. Via the centralised system, the (health) authorities have access to all the contact data of people who have tested positive, but those data also include contacts with people who do not run any risk of infection. That is more personal data than strictly necessary for source and contact investigation. The makers of TraceTogether do not consider this a problem but see it precisely as an advantage that it is decided at the central level which contacts are regarded as risky. This reportedly makes it possible to calibrate the system for false positive or false negative reports.[65]

Decentralised data processing

The decentralised model, known as 'Decentralised Privacy Preserving Proximity Tracing', or DP3T[66] for short, was developed in response to concerns about the privacy failings of the centralised model. The decentralised model also has a centralised system, a back-end, but that does not have access to personal data and functions mainly as a hatchway for the mobile COVID-19 app.

[65] https://bluetrace.io/static/bluetrace_whitepaper-938063656596c104632def383eb33b3c.pdf

[66] https://github.com/DP-3T/documents/blob/master/DP3T%20White%20Paper.pdf

The COVID-19 app on an individual smartphone itself generates a secret encryption key with which a series of time-related, coded smartphone identifications are created. If a user tests positive, the app deposits only the encryption keys in the centralised database. The coronavirus app regularly retrieves the encryption keys from the centralised database. With the retrieved encryption keys, the app reconstructs the smartphone identifications for the past period in which an infection could have been transmitted. The app then uses these to search in the locally stored contact data. The user receives a warning if these smartphone identifications appear in the contact data and the contact was longer than the critical time duration.

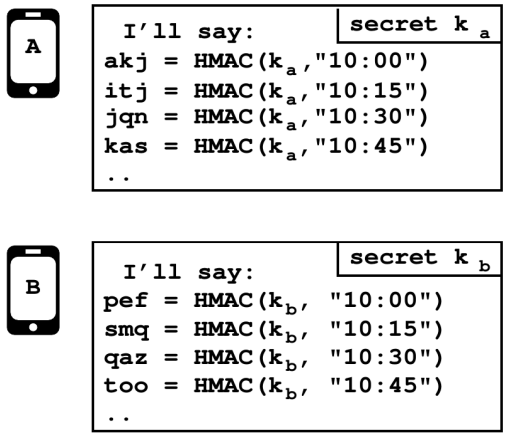


Figure 3. Decentralised model: the HMAC function uses the secret key to create the coded smartphone identifications for 15-minute periods.

Figure 4. Decentralised model: the app retrieves encryption keys from app users who have tested positive and can use these to search in the contacts registered locally.

Privacy by design

The decentralised model of DP3T is an example of 'privacy by design'. The design makes no compromises in terms of privacy and only records the minimum data needed. Mission accomplished. Kudos for that. But then the programming work had to begin in many countries. At the beginning of April 2020, Google and Apple decided to create a joint 'application programmers interface' (API) for contact-tracing apps and in doing so embraced the DP3T design.[67] This initiative was dubbed the Google Apple Exposure Notification (GAEN), reportedly to avoid the term 'contact tracing' so as to increase public acceptance.[68]

GAEN encompasses a feature for COVID-19 apps that is contained in the iOS and Android operating systems. It contains the technical foundations from the DP3T design: the encryption functions and the processing of the Bluetooth Low Energy signals.[69] The payload of the BLE signals is now also equipped with a parameter for distance determination.[70] The joint initiative means that the apps are easily interoperable on both types of smartphones, so they can handle each other's data.[71] The DP3T specifications harnessed convinced many. Moreover, the GAEN feature is an offer that cannot be refused.

The Germans abandoned a centralised model as soon as the failings in privacy protection came to light. The UK's project was initially also based on a centralised model of data storage but was under fire for a long time because of the lack of clarity about the privacy measures, a lack of transparency and dubious tendering procedures. Ultimately, the UK also made a U-turn and went along with the decentralised model.[72] In the meantime, most European countries have opted for the decentralised model and the COVID-19 apps use the GAEN features. This also applies for the CoronaMelder app and the Belgian Coronalert app.

---

[67] Apple and Google are working together to introduce an API for coronavirus apps with Bluetooth. https://tweakers.net/nieuws/165780/.html

[68] https://www.cnet.com/news/why-apple-and-google-are-moving-away-from-the-term-contact-tracing/

[69] https://tweakers.net/nieuws/166750/google-en-apple-maken-eisen-bekend-voor-toegang-tot-corona-api.html

[70] https://tweakers.net/nieuws/166386/.html

[71] The hypocrisy of this position should be pointed out, since Apple itself developed the BLE beacon technology, which is ideally suited for use in monitoring smartphone users.

[72] https://www.reuters.com/article/idUSKCN22807J and https://www.bbc.com/news/technology-53095336.

In conclusion

Apple and Google impose significant restrictions on the use of the GAEN technology. In the app stores, only one COVID-19 app using the GAEN features is permitted per country. The app may not track geographical locations and the provider must be an official health authority. The companies also declared that they will be phasing out the feature after the pandemic. All of this in order to protect the privacy of users and to ensure that the data collected are only used for combating the pandemic.

It is a curious development that Apple and Google now want to protect citizens against the potential abuse of the contact-tracing possibilities. All things considered, with the new Bluetooth facilities Apple and Google added an instrument to the arsenal of digital surveillance technologies. These may be convenient for users, for instance when it comes to getting directions or finding the best discount, but their main function is to track people, profile them and then make them into docile consumers.

The course of affairs with the COVID-19 apps is a stark confrontation with reality, which shows how much states' sovereignty has already been undermined by dependency on Big Tech. The question is whether and how we — the Netherlands, Europe and the free world — want to move forward with this. This big question is not easy to answer but points once again to the fact that technical choices often require a moral weighing of the possibly far-reaching implications these choices have for society. *Great power brings great responsibility*.

A few points for attention

- Centralised or decentralised. With many information systems, centralised data storage is the result of cost or efficiency considerations, or a single database is simply the default. But central data storage is often a result of Conway's Law and is thus a reflection of an organisation that is itself set up in a centralised manner. Nonetheless, sometimes decentralised or compartmentalised data storage is preferable in order to limit the consequential damage caused by data leaks, malfunctions or malware. The recent data leak at the GGD was evidently the result of setting up a national call centre where temporary employees had access to all the data, while the GGDs are organised regionally. Had the call centres been set up regionally, this would already have limited the effects of a data leak.

- Privacy. The digital world is characterised by what is referred to as a 'shifting baseline syndrome'. Once upon a time, in the 1990s, the introduction of cookies was a controversial privacy issue. Now, cookies, scripts and other tracking techniques are standing practice. People were once upset about the Google Streetview vehicles. Now even the municipality drives one around. There was once debate about surveillance cameras in public spaces. Now, these can be found everywhere and incorporate real-time facial recognition software. The debate has gone silent, the reference point has shifted, opting out is no longer an option.

- Opposition. It emerges that a decentralised system is possible for a COVID-19 app even without the GAEN features. A group of German volunteers has, they claim, made the Corona-Warn-App entirely 'Google-free'. This is only possible on Android, because this operating system leaves access to the BLE hardware open.

- Effectiveness. Not much is clear yet about the effectiveness of the COVID-19 apps. Until now, the authorities have been 'cautiously optimistic'. According to the RIVM, between 10 October 2020 and 10 January 2021 a total of 2,601,198 persons were tested, 339,689 of whom emerged to be positive. That is 13.06%. According to the CoronaMelder factsheet, during that same period, 85,688 people were tested after a warning from the app. Of that number, 8,182 tested positive. That is a percentage of 9.5%. So that is a lower percentage than reported by the RIVM for the total number of tests. It is difficult to interpret the figures, but they seem to point to an excess of false positive reports.

4 Germany: Great Expectations and a partially Disillusioning Reality

Rainer Malaka and Kai Rannenberg

Germany was not the first country to offer its residents a Corona warning app. One reason for a later release than in other countries was a major discussion on viable approaches. However, given the size of the project and the number of involved stakeholders, the time until deployment was still quite short. Since June 2020 an app is available and often named as a positive example to combine effectiveness and civil liberties. But despite some notable achievements, there are several weaknesses in the app and its context that require further work.

Early approaches and steps

In Germany, the discussion to develop and deploy an anti-Corona app started in early spring 2020. While some countries made such apps obligatory and also used centralized data collections, this was criticized in Germany. Also approaches to use mobile operators' location data for tracing user movements were discussed. These approaches were criticized for their threat to privacy due to movement profiles and later, as their inefficiency leading to false positives was described: mobile operator location data based on geo-coordinates are often imprecise, especially when buildings have several floors. So, two people being at the same geolocation but in different floors of a building would have been seen as a contact.

Therefore, the discussion moved from movement tracking towards contact-tracing via Bluetooth Low Energy (BLE). Again, the initial plan and its implementation from mid-April 2020 followed a centralized approach for receiving and comparing identifiers and thus identifying contacts. Only after major concerns raised by various international and national stakeholders (including the German Informatics Society),[73] the federal government of Germany changed its direction towards a decentralized architecture on April 26, 2020. However, it did not become fully clear whether the government had decided to choose for the decentralized architecture due to the concerns raised or at least partially due to major delays and

[73] https://gi.de/meldung/gi-unterstuetzt-internationale-stellungnahme-zu-corona-tracing-apps

apparent management issues in the development of an app following the centralized approach.

Corona-Warn-App

Development of the German 'Corona-Warn-App' (CWA)[74] then started on April 28, 2020, and its first version for the general public was released 16 June 2020.[75] The publisher of the CWA is the German Robert-Koch-Institute (RKI), the national central scientific institution in the field of biomedicine. Development was done by German Telekom and SAP.

The CWA follows a decentralized architectural approach based on the Privacy-Preserving Contact Tracing Protocol (PPCP) from Apple and Google using Bluetooth. In addition, all data should only be stored on the local device. All source code is published in GitHub.[76] These measures should raise the acceptance from the users. The DP-3T- and TCN protocols inspired the realization and all source-code is published under Apache-2.0 license.

The main functionality of the CWA is an Exposure Notification Framework (ENF). With this, risks are calculated, positive Corona tests can be recorded and notifications are given to the CWA users.[77] Three web-servers handle information on positive tests, verification and TAN data, and the warning mechanisms separately to avoid linking of information and make it more difficult to trace down individual user data. On the user side, users can enable the risk evaluation which needs BLE to be enabled. This allows for checking potential contacts with other users who are identified as high-risk users, when for instance tested positive. The protocol uses temporary exposure keys (TEK) to ensure anonymity. The CWA has been published in multiple languages (today more than 20). It shares some compatibility with other apps across Europe using interoperable Bluetooth codes.

Acceptance

According to the RKI, the CWA has been downloaded more than 25 million times[78] as of the fifth of February, with 56% downloads via the Google Play store and 44%

[74] https://www.coronawarn.app/en/

[75] https://www.bundesregierung.de/breg-de/themen/corona-warn-app/corona-warn-app-englisch

[76] https://github.com/corona-warn-app

[77] https://github.com/corona-warn-app/cwa-documentation/blob/master/solution_architecture.md

[78] https://www.rki.de/DE/Content/InfAZ/N/Neuartiges_Coronavirus/WarnApp/Archiv_Kennzahlen/Kennzahlen_05022021.pdf

via the Apple store. Given the German population of over 83 million this is not indicating nationwide coverage. In addition, the number of downloads does not mean that these 30% potential users of the CWA are actually distinct active users. Some of these downloads may have been uninstalled or the CWA may have been installed more than once by the same user, e.g. due to the use of several devices or the changes of devices. As the decentralized concept does not give access to usage data, it can only be guessed how many people actually use the CWA. A cross-country study indicates that around 40% of the users of the CWA may likely uninstall it again.[79]

With a relatively broad consensus on the integrity of the CWA it may be surprising that not even a quarter of the population is using the app. This seems to be a strong contrast to the effects of the pandemic that caused deep cuts into the daily lives of many people like lockdowns, school closures, or the loss of family members. So, one may have expected that with close to 90% of the population being smart phone users,[80] almost all of them should have an interest in using the CWA for containing the virus and would follow that interest. However, several weaknesses in the CWA and in its context (see next section) give reason to the assumption that the actual number of users who use the CWA continuously, consistently, and in a fully functional way may be much smaller than 25 Million.

Possible Reasons

One type of reasons for people not installing the app, not using it, not using it in a functional way, or removing it are hindrances caused by restrictions or weaknesses of the device technology and the distribution of the (operating system) software, that the CWA needs to function:

- The BLE capability is not implemented in a number of older devices. To build an app with reliable and battery-saving functionality and the required privacy protection, the developers employed some of the latest features on mobile phones that are not present in older models.

[79] Altmann S, Milsom L, Zillessen H, Blasone R, Gerdon F, Bach R, Kreuter F, Nosenzo D, Toussaert S, Abeler J, Acceptability of App-Based Contact Tracing for COVID-19: Cross-Country Survey Study, JMIR Mhealth Uhealth 2020;8(8):e19857, doi: 10.2196/19857

[80] https://de.statista.com/statistik/daten/studie/459963/umfrage/anteil-der-smartphone-nutzer-in-deutschland-nach-altersgruppe/#:~:text=Rund%2097%2C3%20Prozent%20der,noch%20auf%2052%2C1%20Prozent.

- Relevant functionality is not available in older operating system versions. For example, Apple made the necessary OS functionality available to iOS 12 only 2021-02-10 (while trying to push users to iOS 14 and before requiring at least iOS 13.7 and before iOS 13.5). Given the sometimes disastrous experiences following the update of iOS, many users are reluctant to do so, e.g. beyond iOS 12.4. Even now that iOS 12.5 was made available it is not available for all iOS 12.4 users through the usual channels. Only iPhones that cannot operate iOS 13 or iOS 14 at all get easy access to iOS 12.5. Others still need to be upgraded to iOS 14, even though this may have unwanted effects on performance or compatibility with other (deemed important) apps.
- In many devices an active Bluetooth module leads to significant higher energy consumption and therefore users switch it off to save battery power.
- A network connection is needed at least sporadically in order to update the daily key for the CWA, but some users in particular while travelling disable mobile data and thus disable the app.
- A more organizational frustration was caused by the lack of a consistent treatment of users reporting an exposure and asking for support. Especially access to testing facilities was reported difficult for people who reported an exposure. So, some users were confronted with the fact that CWA reported a problem, but the next steps were unclear. Later, when the 2nd wave began, it became clear pretty soon, that the health authorities were not really capable to follow up on individual 'risks' contacts, which mooted the effect of contact tracing.
- A reason for disabling Bluetooth may also lie in security and privacy concerns not related to the CWA itself but to other apps or companies like Google or Apple possibly able to use this connectivity for information gathering. Moreover, not all potential users seem to believe the governmental assurances, after it needed a lot of pressure to it towards this way. A longitudinal study is investigating which factors determine the use of the CWA and (whether/how) its users and non-users can be clustered based on political beliefs and personal characteristics.[81]

Effectiveness

As no real usage figures are available it can only be guessed to what extent the CWA has a statistical chance to make a difference in the spread of the Pandemic.

[81] https://www.m-chair.de/index.php/research/current-projects?view=project&id=29

What is available from the RKI is that since the launch of the CWA, 7.9 Mio test results were registered including 227,985 positive test results. With ca. 2.3 Mio positive tests up to the same date, this includes ca. 10% of the cases.

With only one third of the population using the CWA, one can estimate the number of actual warnings that could indicate a correct warning as below 3% of the real cases. So far there is no clear evidence how effective the CWA can be and what coverage is needed for its effectiveness. Even though some studies suggest that small numbers of users like those found in Germany might already lead to useful results, the assumptions are not applicable to the situation in Germany.[82]

Conclusions

Even though the CWA was optimized for large acceptance in the German population, it did not prove to have a great impact in an effective containment of Covid. The surge in fall 2020 and winter 2020/2021 was not much affected by the use of the CWA. It could not avoid the restrictive measures such as lockdowns of businesses, restaurants, school closures and travel restrictions. Besides the reasons discussed so far, there are also motivational factors for using the CWA that would – in the best case – just have no effect and in other cases lead to interaction caused by (bad) news about an infection risk and the corresponding threats.

This leads to a low individual motivation to use the CWA on a voluntary basis. In order to raise motivation to use the CWA, outside stimuli like bonuses for its use (positive) or penalties for not using it (negative) would be one way to go. E.g., people could get value in the app stores for using the CWA. Employers or state officials could make it mandatory to use it e.g. in schools or public space. However, making the use of the CWA mandatory would also make it mandatory to use a compatible smartphone in a way that the CWA can work. This type of pressure would need a justification that is hard to imagine, given that the effectiveness of the tracing approach is limited to relatively low infection rates, that allow a targeted reaction to 'infection bubbles'. Measures targeted to e.g. hot spots of infection seem more focused.

Another motivational trigger could be done by a combination of added values in the CWA such as gamification approaches. As gamification has been

[82] Hinch et al., 2020, Effective Configurations of a Digital Contact Tracing App: A report to NHSX

proven to be successful in many health-related interactive systems,[83] it could also be a good motivational factor for certain target groups of CWA.

Lessons learned and further work needed

From the experience gained further work is needed in the following areas:

- Results and other information made available by the CWA should be picked-up effectively and efficiently by the 'rest' of the health system.
- Better availability of the CWA, respectively the underlying (OS) software; in the long run this may require more influence on the market for mobile OS.
- Motivational stimuli: In particular many young users could be attracted and motivated via more playful and gamified approaches.

[83] Malaka R. (2014) How Computer Games Can Improve Your Health and Fitness. In: Göbel S., Wiemeyer J. (eds) Games for Training, Education, Health and Sports. GameDays 2014. Lecture Notes in Computer Science, vol 8395. Springer, Cham. https://doi.org/10.1007/978-3-319-05972-3_1

5 Corona-appathon: Wunderkind or Total Loss?

Serge Wallagh

It is April 2020. The infectious disease Covid-19 is ravaging the Netherlands as well. Efforts to combat the spread are dominated by lack of clarity. Suddenly, a contact-tracing app appears to be an important element; a mobile application that sends people a notification if they have been in the vicinity of a person who has tested positive. But what does this kind of app look like? And how can it be built quickly and yet securely? The cabinet decides to make the first step into a competition. A so-called 'appathon', by analogy to a 'hackathon', in which participants come up with software solutions for a problem in a very short timeframe. On 11 April 2020, the competition is published on TenderNet. The deadline for submission is 14 April: just three days later. The best submissions will then have to give a presentation on 18 and 19 April. Around 21 April, it emerges that the approach has not yielded anything: all 660+ submissions are rejected over the course of several rounds. Was the appathon doomed to fail from the start, or can something be learned from the creative approach?

Variation on a hackathon

The concept of an 'appathon' did not exist. This word was invented for the occasion. In terms of setup, definition and execution, however, it very closely resembled what is referred to as a hackathon, with one big difference. Hackathons are a common occurrence these days. They are events in which teams of participants work non-stop to develop solutions within a very short timeframe for cases presented to them, with the aim of coming up with an innovation. In this context, 'hacking' does not ~~so much~~ mean breaking into computers, but creatively seeking out the new possibilities of a system.

The appathon is a variation on this: a coming together of experts in programming, data collection and cybersecurity in order to thoroughly test apps

and together to seek (technological) solutions for any shortcomings[84]. The big difference is therefore that in a hackathon, the participants create something on-site, which is not expected to be a finished product. With the appathon, the participants were required to present a ready product, with all the expectations this entails.

Chronology of an eventful week

Back to 11 April 2020, the day the appathon was officially announced. Minister De Jonge (Public Health, Welfare and Sport, VWS) officially announces that there will be an appathon[85]. On the one hand there was enthusiasm, on the other, a storm of criticism. The enthusiasm came mainly from the companies, with over 660 registrations. After a preselection process, 63 proposals remained, which were assessed by 67 experts in the areas of epidemiology, healthcare, privacy, information security and ICT. With reference to the advice from these experts, seven participants were selected who would fight it out on 18 and 19 April 2020. The central government website optimistically reported that these apps satisfied the requirements stipulated for, among other things, privacy, data and information security and user-friendliness.[86]

There was also a great deal of criticism. Even before the appathon was announced, a broad coalition of scientists and privacy experts drew up a list of requirements on 8 April 2020. [87] They insisted that the app must be transparent, fully anonymous, voluntary and user-friendly, without commercial ulterior motives, and under the direction of independent experts. If not, then this coalition would fiercely oppose the implementation of the app.

After the announcement, the political party D66 asked the minister whether he thought 14 April 2020 was a realistic deadline for the experts and companies to prepare a proper response to the tender (after all, the announcement was on 11 April 2020) and why the government was calling for the submission of already existing, fully developed and working solutions. "Does this not wrongly exclude innovative solutions that are not fully developed at this point?"[88]

---

[84] Source: www.taalkbank.nl

[85] https://www.tenderned.nl/tenderned-tap/aankondigingen/192421

[86] https://www.rijksoverheid.nl/actueel/nieuws/2020/04/17/zeven-apps-doen-mee-aan-publieke-test-komend-weekend

[87] https://www.veiligtegencorona.nl/

[88] https://zoek.officielebekendmakingen.nl/kv-tk-2020Z06655.html

The appathon itself was extremely intensive. The competition began with the online presentation by the seven different teams to experts from both within and outside the government. The first day of the appathon concluded with a question and answer session and review and a short presentation by the teams. The following day, the appathon picked up again with a presentation, after which the teams had until 4 PM to make further modifications. The day ended at 4 PM with final demonstrations by the teams. The appathon was viewed by approximately 90,000 people; 24,000 gave their opinions on the proposals via a special central government website. The total costs incurred by the central government for the appathon amounted to approximately €400,000.[89]

Results

On 19 April 2020, the final report from KPMG was published,[90] commissioned by the Ministry of VWS. Perhaps indicative of the time pressure, the report devoted almost four pages to setting out the limitations of the audit. The report is very critical. The application developers did not generally use any secure coding principles, so that widely known and therefore expected security measures were not implemented, the underlying infrastructure had (serious) vulnerabilities that could easily have been avoided, data were often stored without encryption and general measures to promote code quality were encountered to only a limited extent. Reading between the lines, one can gather what is being said here: *from a technical perspective, the apps are unusable*.

There are legal issues as well. The State Advocate asserts that based on the documents assessed, none of the proposals were found to fully comply with the starting points formulated. Nor could it be determined that all the requirements of the General Data Protection Regulation (GDPR) were satisfied. They were unable to determine that full anonymity was guaranteed in any of the proposals. [91] The Dutch DPA added that the seven app proposals were insufficiently worked out, in part because the Ministry of VWS had not set out the frameworks clearly enough.

[89] Parliamentary document 35493, no. 3.

[90] Security test of potential Coronavirus apps, Ministry of VWS, A2000020142, KPMG Final Report, 19/04/2020

[91] Public summary of privacy analyses of source and contact investigation apps, Gerrit-Jan Zwenne and Marte van Graafeiland, Pels Rijcken, State Advocate, 19 April 2020

Because of this, it could not be assessed whether the protection of Dutch residents' sensitive data was sufficiently guaranteed.[92]

On 21 April 2020, Minister De Jonge has no choice but to officially conclude that the appathon was a failure. He states that the visible efforts of all of those involved in the run-up and during the appathon gave rise to a broad societal debate and that he was pleased with that. And also with the critical notes that were heard. In addition to the technical problems, the minister also concludes that it has become clear that the requirements that the GGD has stipulated for the digital support of source and contact investigation need to be more precise. His final conclusion is clear: "Partly on the basis of the conclusions of KPMG, the State Advocate, the Netherlands Institute for Human Rights and the Dutch DPA, I have decided not to grant the contract for the use of one or more specific solutions as have been submitted to date." [93]

Aftermath

All the attention on this special approach to the ICT project disappeared as quickly as the appathon had arisen. After the letter to the Lower House of Parliament on 21 April, there was little further communication about the appathon. The Minister of VWS then put together a team of experts to start developing the definitive coronavirus contact-tracing app. A number of the key critics of the coronavirus app were expressly included in this. During deliberations on the Temporary Act on the COVID-19 Notification Application in September 2020 in the Lower House of Parliament, the minister revisited the appathon. "When I look back on that myself, I should have made it clearer that we were starting a search for something whereby we could not be certain whether it would actually produce an app at the end of the weekend. I think that because of that, expectations were too high and the result was too disappointing."[94]

Conclusion

The appathon did yield results, however. Firstly, the initiative contributed to the drafting of the *schedule of requirements* for the definitive coronavirus app. Stringent requirements were formulated, based in part on the strong criticism. An army of

[92] Research report source and contact investigation apps, Dutch DPA, 20/04/2020

[93] COVID-19: Update stand van zaken [COVID-19: Update on state of affairs], H. de Jonge, Reference: 1677140-204449-PG, 21-04-2020

[94] Proceedings h-tk-20192020-96-6, 02-09-2020

almost fifty experts were also appointed from the domains of information security, privacy, fundamental rights and national security who were involved in the development process, along with the Dutch Data Protection Authority, the Netherlands Institute for Human Rights, the National Cybersecurity Centre and the National Coordinator for Security and Counterterrorism.

Looking back, we see other positive points as well. Dutch software developers, united in Code for NL, hope that this approach is an impetus for a future model for assessing technological solutions and that this can result in optimal cooperation between government and society.[95] Amnesty International even goes a step further and states that the appathon shows that our democracy is alive and kicking. The government clearly listened to advice from all corners of society, although they do still feel that even the latest coronavirus app does not meet their requirements.[96] [97]

To conclude with the words of Minister De Jonge: "After the appathon, it was impossible to continue with the process in any way but transparently. After all the turmoil, the bumpy start, there really was only one way: the very highest requirements had to apply in relation to privacy, security, accessibility and communication and it had to be entirely voluntary."

Some considerations

- The first appathon in the Netherlands was too hasty in terms of setup, involved unrealistic expectations and simply wanted to achieve too much too fast. Its likelihood of success was minimal as a result.

- In this case, the appathon also ensured robust requirements for the definitive contact-tracing app for COVID-19, which in turn helps bolster public support for this mobile application.

- The cooperation between many parties, which started during the appathon and continued with the development of the definitive coronavirus app, contributed to a better end-product from a technical, legal and ethical standpoint.

[95] https://codefor.nl/appathon/

[96] https://www.amnesty.nl/wordt-vervolgd/corona-surveillance

[97] https://www.veiligtegencorona.nl/analyse.html

- An appathon can give smaller software developers the opportunity to present themselves to the government. That is often much more difficult for these parties in the context of regular tendering procedures.

- The appathon format could lend itself for the beginning phase of other government ICT projects, on condition that it is carefully planned and includes realistic timelines. This format can yield more transparency, innovation and renewal. And perhaps prevent the failure of ICT projects to some extent. The appathon format offers enough prospects for this to warrant further exploration.

6 Strict European tendering rules, even in times of crisis?

Menno de Wijs

The central government, including its ministries, is required to conduct a European tendering procedure for contracts with a value in excess of €139,000.[98] How did the Dutch government deal with this requirement when having the CoronaMelder contact-tracing app developed? Since the procurement law is European law, this raises the question of whether this course of action is similar to that taken by other European countries. After all, the Netherlands was not the only country facing this crisis, and this provides a unique possibility to compare the working method of the Dutch government with that of other European countries from the perspective of procurement law. Aside from limited implementation differences, the legal framework is identical, after all.

Time-consuming process

Tendering takes time, a lot of time. The publication of tendering documents — which is often the start of a tendering procedure for the market — is often preceded by months of work. Once the procedure has begun, there are also statutory (minimum) time periods that must be observed. For instance, a public tendering procedure has a minimum lead time of at least 45 days.[99] It is only once the procedure has been fully completed that a contract can be definitively awarded. As long as one of the unsuccessful tenderers has not initiated proceedings to challenge the proposed award decision that is. The Public Procurement Act stipulates that the proposed award decision cannot be implemented during summary proceedings. The contract cannot be signed until these proceedings have been concluded, and the court judgment allows definitive award to the winning tenderer. That is the starting shot for the work activities to commence.

[98] This is the threshold for services and supplies to central governments (the threshold for local governments is €214,000). For 'works', a considerably higher threshold of €5,350,000 applies and, moreover, there are another several variations in relation to the thresholds.

[99] Section 2.71 Public Procurement Act.

Legislation and regulations

It requires no explanation that at times of crisis, this kind of time-intensive process is not desirable and may even be impossible. If the dikes are breached, they must be repaired quickly; there is no time to await the outcome of a tendering procedure. That brings us to the legislation and regulations. Despite the fact that public procurement in the Netherlands dates back to 1815, the Dutch Public Procurement Act is primarily a combination of three European directives. Exceptions to the obligation to issue calls for tenders must be applied with extreme restraint. Was this kind of exception perhaps invoked for the development of the CoronaMelder app?

Tendering procedure for the coronavirus app?

Minister De Jonge announced during a press conference on 7 April 2020 that the cabinet would be starting work on two mobile apps. As described elsewhere in this collection, from that point on, things moved quickly. The media reported on an extremely rapid tendering procedure, and reference was also made to a 'tender' during parliamentary questions.[100] The documents for this were published on Saturday, 11 April 2020, and the period for submitting tenders closed at noon on Tuesday, 14 April. It could hardly have been quicker, especially since Monday, 13 April was Easter Monday.

But did this involve a tendering procedure? An examination of the extensive letter from Minister De Jonge shows that he did not mention a 'tender', but a consultation.[101] The confusion may have arisen as a result of an announcement on TenderNed,[102] the government platform on which all tender-related notifications must be published.

Market consultation

Examination of the announcement indicates that it did not involve a tendering procedure, but a market consultation. Lack of knowledge of public procurement

[100] https://www.tweedekamer.nl/kamerstukken/kamervragen/detail?id=2020Z06655&did=2020D14737

[101] Letter from Minister De Jonge to the Lower House of 16 April 2020 https://www.rijksoverheid.nl/regering/bewindspersonen/hugo-de-jonge/documenten/kamerstukken/2020/04/15/covid-19-update-stand-van-zaken

[102] Announcement dated 14 April 2020, https://www.tenderned.nl/tenderned-tap/aankondigingen/192421

law could wrongly give rise to the impression that this is a tendering procedure. A market consultation is an instrument that can precede a tendering procedure. During a consultation, the market is asked for information in relation to a proposed tendering procedure. In the market consultation for the coronavirus app, the question was what was already available on the market.[103] During the testing — dubbed an 'appathon' — it emerged that none of the solutions was satisfactory.[104]

The minister subsequently decided that the government would develop an app itself. This was later called: the CoronaMelder.[105] The development team put together consisted of internal and external experts. No publication about the award of a contract to an external party can be found on TenderNed. It is possible that the value of each individual contract awarded to the experts did not exceed the threshold value, but it is also conceivable that these activities were brought under a framework agreement for ICT services that had already been awarded and published. Incidentally, examination of the Official Journal of the European Union — in which all tendering procedures are published — indicates that various countries make no mention whatsoever of a contract for the development of their contact-tracing app.

Tendering of 'coronavirus contracts'

What if the contract for the development of the CoronaMelder had been entirely awarded to an external party? Would a European tendering procedure be followed in that case? That is simple to answer. First and foremost: that contract would be subject to tendering. The development costs of the CoronaMelder app, in the amount of approximately €5, amply exceed the threshold value.[106]

As indicated above, there are a limited number of exceptions to the obligation to call for tenders. One of those is the exception on account of extreme

[103] According to Minister De Jonge by letter of 16 July 2020, https://zoek.officielebekendmakingen.nl/kst-25295-460.html

[104] According to Minister De Jonge on 22 April 2020, https://zoek.officielebekendmakingen.nl/kst-25295-277.html

[105] Minister De Jonge by letter of 24 June 2020, https://zoek.officielebekendmakingen.nl/kst-25295-428.html

[106] See chapter 10, Financial aspects of COVID-19 apps

urgency.[107] The contract may be awarded directly in that case.[108] Important conditions are that (i) because of extreme urgency, the time periods of a tendering procedure cannot be observed, (ii) the particular event could not have been foreseen by the tendering authority, and (iii) the event also cannot be attributed to that tendering authority. The outbreak of the coronavirus is an unforeseeable event, one that cannot be attributed to the tendering authority and which could, therefore, justify an exception to the obligation to tender.

Shortly after the coronavirus arrived in European territory, the European Commission issued a guideline.[109] In this, the European Commission stated that the coronavirus could justify invoking the urgency exception. The Dutch government took careful note of this communication and applied the urgent procedure repeatedly during this crisis. For example, for the purchase of facemasks[110] and artificial respiration equipment,[111] but also for the hosting of the coronamelder.nl website.[112]

Incidentally, this was being done throughout Europe: for instance, the United Kingdom relied on this exception in developing its version of the CoronaMelder.[113] The fact that in this situation, the exception was invoked is, in my view, certainly acceptable and would stand up to judicial scrutiny. The development of the CoronaMelder app as well could successfully be covered by this exception.

Expiry date for urgent procedures

A critical comment is called for, however. At the end of 2020, the coronavirus had been in the Netherlands for 10 months. The longer a crisis situation lasts, the more imminent the expiry date for urgent procedures. The enormous demand for personal protective equipment in March 2020, for example, was unforeseeable. That has changed in the meantime, however, and one could take the position that the current demand was foreseeable. The urgent procedure may only be used for a bridging period: contracts may not last longer than the time period necessary to

[107] Section 2.32(1)(b)(c) Public Procurement Act.

[108] Private award (direct award) is designated in the Public Procurement Act as a 'negotiated procedure without publication', according to section 2.32 Public Procurement Act.

[109] Communication from the European Commission dated 1 April 2020, 2020/C 108 I/01

[110] https://www.tenderned.nl/tenderned-tap/aankondigingen/213290;section=1#detail-publicatie:linkS4

[111] https://www.tenderned.nl/tenderned-tap/aankondigingen/206592

[112] https://www.tenderned.nl/tenderned-tap/aankondigingen/213290;section=1

[113] https://ted.europa.eu/udl?uri=TED:NOTICE:280701-2020:TEXT:EN:HTML

follow a tendering procedure. Nevertheless, facemasks were still largely being purchased on the basis of the urgent procedure in December 2020. The market must wonder whether that is still lawful and until what point in time that remains lawful.

It is important in this context that in the event of urgency, an accelerated procedure is also possible. This could be considered a regular tendering procedure in which the minimum lead time can be shortened from 45 days[114] to 15 days.[115] It is only if this lead time is too long, in view of the urgency, that the actual urgent procedure may be used. The contracting authority must justify why this accelerated procedure is insufficient. Judicial decisions show that even before the coronavirus crisis, this did not always go well.[116] In that case, the judge issues an injunction against performing the contract. It is important, therefore, that contracting authorities and the market take a critical view of (excessive) long-term use of the urgent procedure.

That does not apply only for the Netherlands. In Germany as well, a critical view is taken of excessively long use of the urgent procedure. In mid-2020, a German judge stated in an interview that much of the procurement from summer 2020 onwards should already be taking place via the *accelerated* procedure.[117] The long-term demand was already foreseeable at that point.

Conclusion

As time passes by, the chance of successful reliance on the urgent procedure decreases for many projects. For various contracts, this expiry date has even already arrived (some time ago). It is understandable that the tendering aspect fades to the background during urgent situations. Minister De Jong stated in September 2020 in relation to all COVID-19-related purchasing that the tendering dossiers were not all in order, but that the purchases did all fall under the urgent exception discussed and that dossier formation was being worked on. [118] That lack of dossier formation

[114] Section 2.71 Public Procurement Act.

[115] Section 2.74 Public Procurement Act.

[116] District Court Noord-Nederland 21 June 2019, ECLI:NL:RBNNE:2019:2681, para. 4.12.3.

[117] https://www.juris.de/jportal/nav/juris_2015/aktuelles/magazin/corona-vergaberecht.jsp

[118] Letter from De Jonge dated 21 September 2020, Parliamentary Documents 25 295, no. 542:
'For instance, the ministry of Public Health, Welfare and Sport has, with regard to the procurement/purchases that the ministry itself has made, set up the action to still gather together all

must be informed by the unexpected 'demand' and not by insufficient procurement capacity. In my view, contracting authorities must henceforth be extremely self-critical with respect to a desired reliance on the urgent procedure or accelerated procedure. The mere fact that the market has not (yet) intervened does not, after all, make the award lawful.

In conclusion

- A brief search of the Official Journal of the European Union shows that in 2020, at least 500 coronavirus-related contracts were directly awarded by European countries without tendering procedures.[119]

- From the perspective of procurement law, this is the first time that a crisis situation has resulted long term in repeated reliance on the urgency exception throughout Europe.

- For this reason alone, after the coronavirus pandemic has passed, the correct or incorrect use of the urgency exception will undoubtedly have to be evaluated. The biggest pitfall at this point is a defective (i.e. standard) justification for application of the urgent procedure, as a result of which the urgent procedure is used while the accelerated procedure would suffice. That seriously restricts competition and could result in government funds not being spent efficiently. So be alert.

those relevant documents that should be in a procurement dossier. The more complete a dossier, the smaller the likelihood of uncertainties.'

[119] https://ted.europa.eu/TED/search/searchResult.do

7 Network and information security: apps that are secure by design?

Paul Oor

By the end of 2020, there had been more than 1.5 million searches on Google for 'Coronavirus app privacy'. If we replace 'privacy' with 'security', the number of results even increases to four million. The statistics give an indication of the topics on which citizens feel inadequately informed. This enormous interest in the security of an app is striking. After all, virtually everyone has a smartphone, equipped with a great many preinstalled mobile applications. But all these apps, plus the software downloaded later, almost certainly receive just a fraction of the attention to security compared to the contact-tracing apps for combating COVID-19. What is the underlying reason for the widespread demand for information, whereby the Dutch central government is, nota bene, the party commissioning the app? Is trust in the security of an app henceforth a deciding factor in the choice for and acceptance of a mobile application? Can we realise and subsequently demonstrate the security of apps and related system (network) connections? The answer is yes. This can be done by explicitly devoting attention to security and reusing the development and test process for applications and systems that have already proven their effectiveness in the past.

More than regulatory compliance

Legislation and regulations impose increasingly stringent requirements for the security of the information systems of businesses and governments. Appropriate technical and organisational measures are not without obligation; not for apps either. The General Data Protection Regulation (GDPR)[120] applies, but the Network and Information Systems Security Act (Wbni[121]) also requires explicit attention for

[120] https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/beveiliging/beveiliging-van-persoonsgegevens

[121] https://wetten.overheid.nl/BWBR0041515/2020-07-15

system and therefore app security. In April 2020[122], an innovative application[123] development programme was announced: the 'appathon'. An open public/private cooperation to develop a contact-tracing app, which would ultimately be called the CoronaMelder. Although none of the solutions presented fully satisfying expectations, knowledge and experience was amassed. In addition to functionality and effectiveness, the aspects of security and privacy[124] dominated the discussions and decision making.

The Dutch Data Protection Authority[125] quickly indicated it could not give an opinion because the privacy frameworks of the app were not sufficiently defined. In short, privacy and security aspects had not been included in the design requirements, or in any event had not been included sufficiently, even though this was essential for positive assessment by the privacy regulator. A doubtful regulator is never good for trust in and acceptance of a system. Especially if that system processes information on a device that plays a major role in our personal life 24 hours a day.

In the entirely new development programme that followed, therefore, even more emphasis was put on privacy and security during the app development. Ultimately, trust was restored and the app became available nationwide in October 2020. Due in part to a successful Data Protection Impact Assessment (DPIA),[126] the publication of the source code and extensive security tests to validate the security of the app. It was clear; there would be no acceptance of this kind of app without trust in its security.

Secure apps? How?

Trust in the security of an information system, of which apps are also part, proved important for acceptance. In the development of traditional systems, that trust is a matter of clear frameworks and design requirements. While 'agile',[127] supported by 'devops',[128] now also facilitates responsible development based on progressive

[122] https://nl.wikipedia.org/wiki/CoronaMelder

[123] https://nl.wikipedia.org/wiki/Mobiele_app

[124] This article focuses on the security of apps; privacy aspects are discussed elsewhere in this publication.

[125] https://autoriteitpersoonsgegevens.nl/

[126] Data Protection Impact Assessment: https://autoriteitpersoonsgegevens.nl/nl/zelf-doen/data-protection-impact-assessment-dpia

[127] https://en.wikipedia.org/wiki/Agile_software_development

[128] https://en.wikipedia.org/wiki/DevOps

insight. Unlike traditional information systems, apps involve a lot of dynamics. After all, apps can be launched and maintained rapidly and continuously, to a large extent automatically. Without or even with limited intervention by the end user.

Security by default and design

Apple[129] and Google[130] quickly realised that trust in the security of apps was crucial for their earning model. Under pressure from the market, both have since imposed explicit security requirements on the providers of apps before they make apps available via their app stores. The security of the devices[131] [132] that function as the platform on which these apps run, smartphones and tablets, is also constantly being improved. It is technically possible to develop and distribute apps outside these channels, but, in my view, that is complex and undesirable. After all, in that case no use is made of the security measures from Apple and Google, while these measures now play a major role in inspiring trust among app users. At the same time, the approval process is now so mature and affordable that app development still remains feasible for smaller parties and private individuals.

In general, the intrinsic security of apps itself seems to have matured, especially in combination with automated updates and extra measures by the app provider. The security of apps now seems so well provided for that apps are now widely accepted in all sorts of business-to-consumer or even government-to-citizen processes. Banking using apps [133] is regarded as more secure than telebanking via a computer, and using government services that rely on the DigiD app for authentication has become commonplace.

Front door lock

Many end users still have the perception that the data presented to them on a phone are also actually stored on the device. In most cases, however, those data are on an operating system, often in the public or private cloud.[134]

Although a user name and password are still relevant, the inseparable relationship of the smartphone and its user have had a positive influence on the

[129] https://en.wikipedia.org/wiki/IOS_app_approvals

[130] https://www.android.com/safety/

[131] https://safety.google/

[132] https://support.apple.com/guide/security/app-security-overview-sec35dd877d0/1/web/1

[133] https://www.veiligbankieren.nl/veiligheid-betaalproducten/mobiel-bankieren/

[134] https://cloudsecurityalliance.org/blog/2015/10/26/the-definition-of-cloud-computing/

secure unlocking of these data via apps. In addition to *what you know* (password), the device is now so personal that the 2-factor question from an app, *what you have*, can now be primarily answered via the smartphone. Biometric recognition such as a fingerprint, facial recognition or iris scan provides a high degree of certainty of identity when logging in. And if the device is lost or falls into the wrong hands, it can be rendered unusable remotely relatively quickly.

Nonetheless, there are still limitations: if the user and his device travel internationally, security is determined geographically, depending on the country (regime) where the user is. After all, at more and more border crossings you are being forced (even in the US) to give your password, and you are forced to briefly surrender your device to 'officials'. If you also make use of the network in all sorts of countries, you know that traffic via that network is compromised and your device can even become compromised that way. There is good reason why international companies provide their (important) business travellers, athletes, etc with a 'new and clean device' before departure and that this device is immediately collected upon return, sometimes searched and thereafter directly reset to the factory settings or even, on occasion, destroyed.

Why doubts?

Convincing an app user of the value of an app is usually a matter of good marketing. After the question "what does it do for me?" is answered, follow-up questions about security and privacy are hardly ever asked these days. Upon the introduction of the CoronaMelder app, this question did arise quickly; also because the usefulness and consequences for the *individual* user are not immediately clear. Granted. During the coronavirus crisis, everything changed. General uncertainty, the accelerated digital transformation and disinformation certainly played a role in the initial lack of trust in technological aids,[135] such as the CoronaMelder app.

Thanks to the discussions about the CoronaMelder, a large percentage of the population has now become acquainted with the security aspects of apps. It is logical that people will ask more questions in the future about the security of mobile applications. We have our smartphone with us nearly all the time, and, with apps and in combination with wearables and the Internet of Things, it offers us more and more functionality. The number of apps and the competition among providers is growing enormously. It is logical that the security and reputation of apps and the providers will play a more important role in choosing an app. Albeit

[135] https://techtegencorona.nl/

on the basis of trust, not on the basis of substantive knowledge. The lessons learned from the distrust surrounding the development of the CoronaMelder app are important for every app developer.

Trust is good, knowledge is even better

Questions about the security of an app are often answered with: 'it depends', followed by a more detailed and complex explanation if requested. Technical developments are taking place rapidly and are only fully understood by a small percentage of society. In practice, only a relatively small group of specialists with sufficient (technical) expertise can assess the security of app systems. And if the opinion is formed by just a small group of people and topics become too complicated, disinformation is given an opportunity and it is essential to proactively gain people's trust.

In every app development process, the developer, along with marketing and communication, must ask all (!) the questions that users could ask. Even the somewhat far-fetched questions and 'evil user stories'.[136]

In conclusion

Thanks to the steep learning curve in the weeks after the appathon, during which attention was indeed explicitly devoted to the security concerns, criticism of the CoronaMelder app has since largely fallen silent. We learned therefore that in the successful development of apps, for collecting data (app as sensor) and providing (reliable) information via apps, early attention to security by design by default is necessary and all the traditional rules for Secure Software Design[137] remain fully in force.

In short, alongside the earning model — or, in the case of the CoronaMelder, the desire that as many people as possible use the app — and functionality, security by design by default[138] must be explicitly included throughout the entire development process. This prevents an app from having to be on the defensive when it is launched and avoids acceptance being limited because of lack of trust.

[136] https://www2.slideshare.net/AnneOikarinen1/evil-user-stories-improve-your-application-security

[137] https://www.cip-overheid.nl/productcategorieën-en-worshops/producten/secure-software/

[138] https://www.digitaleoverheid.nl/nieuws/zo-bouwen-wij-software/

Some considerations

The range of apps on offer is now enormous and the number continues to grow,[139] competition is increasing and developers will have to distinguish themselves by their quality and security. On the basis of this, we make the following suggestions:

- define a policy for the safe development and use of apps;
- design and develop apps as a real information system, under the control of IT; avoid 'shadow IT';[140]
- devote a great deal of attention to Secure App Design; [141] safeguard compliance with legislation and regulations
  organise security tests and work on a response to push back;
- ask communication specialists to develop a clear and unambiguous explanation for end users and anticipate far-fetched questions and scenarios (evil user stories).

[139] https://www.statista.com/statistics/276623/number-of-apps-available-in-leading-app-stores/

[140] https://en.wikipedia.org/wiki/Shadow_IT

[141] https://www.ncsc.nl/documenten/publicaties/2019/mei/01/ict-beveiligingsrichtlijnen-voor-mobiele-apps

8 Privacy and COVID-19 apps

Jeroen van Helden

In April 2020, the Ministry of Public Health, Welfare and Sport (VWS) formulated the first requirements for a future coronavirus app for the purposes of automating source and contact investigation. Privacy protection occupied an important role in that. For instance, in the data processing, it had to be impossible to trace data back to a person and data had to be stored and processed locally on the individual's own phone. Decentrally, therefore. It was also a requirement, of course, that the mobile application was fully compliant with regulations under the General Data Protection Regulation (GDPR), the European privacy law that has been in force since 25 May 2018. The question arises of whether the app ultimately rolled out nationally on 7 October 2020 lived up to the high aspirations for data processing and the protection of our privacy. And: what does the process followed say about the privacy aspect in new ICT projects?

Reports and recommendations

The fact that privacy protection was a central concern in the development of the COVID-19 contact-tracing app CoronaMelder was clearly evident from the large number of reports and recommendations published on this topic. The state advocate carried out a privacy analysis into the proposals submitted during the appathon in April 2020,[142] the Dutch Data Protection Authority produced a number of recommendations, including a voluminous and critical advice on the app,[143] on which the state advocate in turn then gave his thoughts,[144] the explanatory memorandum to the Temporary Act on the COVID-19 Notification Application

[142] Pels Rijcken, Openbare samenvatting privacyanalyses bron- en contactonderzoekapps [Public summary of privacy analyses of source and contact investigation apps], 19 April 2020.

[143] Dutch Data Protection Authority, 'Advies op voorafgaande raadpleging COVID19 notificatie-app' [Advice on prior consultation on COVID-19 notification app], 6 August 2020.

[144] Pels Rijcken, 'Juridische analyse — advies Autoriteit Persoonsgegeven inzake de DPIA van de CoronaMelder' [Legal analysis — DPA's advice on DPIA for the CoronaMelder], 12 August 2020.

largely concerns privacy matters,[145] the Council of State issued advice as usual,[146] the Ministry of Public Health, Welfare and Sport compiled an almost 75-page data protection impact assessment (or 'DPIA', an instrument to identify in advance the privacy risks of a data processing operation),[147] Minister De Jonge (VWS) asked a consultancy firm to issue a second opinion on the DPIA,[148] etc.

What is striking in this volume of literature is that the authors and advisory bodies are virtually unanimous in their opinion that data protection was given thorough and consistent consideration in the design of the app. According to Brenno de Winter, responsible for the security and privacy in relation to the app, the app therefore became a textbook example of applying the principles of privacy by design and privacy by default. Where discussion arose in relation to privacy protection, this was not so much concerned with the technical side of the app, but with the social embedding and legal classification of the digital application. A few points of discussion will be discussed in more detail below.

Does the CoronaMelder app process personal data?

Among the starting points for the coronavirus app drawn up at the beginning of April 2020 by VWS, it was a priority that it should not be possible to trace information back to individuals.[149] For this reason, the CoronaMelder app uses local data storage and various techniques that, in summary, aim to ensure that the data that an app user shares with other users and with the back-end cannot be traced back to individual users.

The keys that app users exchange with each other via Bluetooth when they are in each other's vicinity and which they store on their phones (RPIs) are generated entirely randomly. The same applies for the key that a user sends to the back-end if he or she becomes infected with the virus (TEKs). The keys that the back-end subsequently sends out to all users to inform them about new infections (DKs) are in turn derived from the TEKs. *No substantive data* are exchanged between the parties involved, therefore, not even encrypted data; there is only the exchange of pseudonymised identification keys. Network traffic is furthermore supplemented

[145] Lower House, 2019-2020 session, 35 538, no. 3.

[146] Council of State, Temporary Act on the COVID-19 Notification Application, 19 August 2020.

[147] VWS, 'DPIA COVID-19 notificatie-app' [COVID-19 notification app DPIA], 24 August 2020.

[148] Privacy Management Partners, 'Second Opinion DPIA CoronaMelder App', 19 August 2020.

[149] Letter from VWS to the Lower House, COVID-19 Update stand van zaken [COVID-19 Update on state of affairs], 15 April 2020.

with dummy keys, so that no tracing back is possible, even on the basis of an analysis of data flows.

Based on the data exchanged alone, therefore, it is not possible to trace back to individuals. European privacy law interprets the notion of personal data relatively broadly. Even data that can only be linked to a specific data subject by using *additional data* that are stored separately and securely qualify as personal data to which the GDPR applies in full.[150] But it is difficult to see, for instance, how the GGD could trace a TEK back to a specific person by using additional data. After all, the TEK is a randomly generated code. Nothing more than that. A vulnerability does arise here, however, because together with the TEKs, IP addresses are also sent to the back-end server. Although these are stored separately from the TEKs, this does not rule out that identification keys can still be traced back to individual users. These keys could then still qualify as pseudonymised personal data.[151]

For other reasons as well, a residual risk of tracing back always remains, especially since the government advises us to now limit contact moments as much as possible. If a person stays home alone all day on Monday, with the exception of a 90-minute meeting at the office with an important client, and then receives a notification on Thursday that he came in contact with an infected person on Monday, he can be virtually certain to whom this notification relates. No randomly generated identification key, pseudo-MAC address or dummy key can solve that.

To be on the safe side, the DPIA of the Ministry of VWS therefore takes as starting point that personal data are or can be processed in all phases of the app.

New law not necessary, but indeed desirable

Every processing of personal data must be able to be based on at least one of the six bases cited in Article 6 of the GDPR.[152] Two of these could potentially serve as a basis for the processing operations via the CoronaMelder app, namely 'consent'

[150] *Inter alia*, see recital 26 GDPR and article 4(5) GDPR; CJEU, 19 October 2016, ECLI:EU:C:2016:779 (*Breyer*); Article 29-WG, 'Opinion 4/2007 on the concept of personal data', 20 June 2007; Article 29-WG, 'Opinion 05/2014 on Anonymisation Techniques', 10 April 2014.

[151] Against this backdrop, it was included in the Temporary Act on the COVID-19 Notification Application that it is prohibited to link the IP address to other data.

[152] To the extent the TEKs and DKs qualify as health data, the app must also be tested against the processing prohibition for special categories of personal data contained in Article 9 GDPR. Because of the limited scope of this article, I do not address the discussion concerning Article 9 GDPR, which, incidentally, is similar to the discussion concerning Article 6 GDPR.

(ground a) and 'task in the public interest' (ground e).[153] It emerges from the legislative history of the CoronaMelder app that there was a great deal of discussion between VWS and the Dutch DPA on the question of which of these two bases was the most appropriate.

The Ministry of VWS initially favoured processing on the basis of ground e, because the existing Public Health Act (Wpg) would already provide sufficient basis for that. After all, the GGDs have the statutory duty of conducting source and contact investigation (sections 6 and 14 Wpg), and the minister has, to summarise briefly, the statutory duty of managing the efforts to combat the virus (sections 3 and 7 Wpg). VWS emphasised in this context that there is no set form for source and contact investigation and that this notion should be interpreted broadly. It could also include support via an app.

The Dutch DPA did not agree with this interpretation. In view of the starting point of voluntariness, consent (including the strict requirements that apply for that) should be the appropriate basis for processing operations in connection with the app.[154] In a number of countries, including Germany and Ireland, the consent basis is also used for a national COVID-19 app.[155]

At some point, the Dutch DPA had a change of mind, however. Consent was reportedly not an appropriate basis for the setup of the app, among other reasons because withdrawal of consent or reliance on the right to be forgotten would, in practice, be illusory. The Dutch DPA felt that the existing Wpg also did not offer sufficient basis, however. The minister especially could not derive a basis from that law. According to the regulator, the minister's authority to manage the efforts to combat an epidemic does not yet provide any basis for the minister to himself process personal data. This authority on the part of the minister would have to be anchored more explicitly in the law.

The Council of State felt that a statutory basis for voluntary use of the app was not legally required, but nonetheless expressed the preference, from a constitutional perspective, for a specific legal regulation. The PMP consultancy firm

[153] Also see 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, margin number 29.

[154] This initial advice from the Dutch DPA was not published, but the substance of the advice was evident from two lectures on the coronavirus app, specifically the lecture organised by the Jonge Balie Den Haag on 20 August 2020 and a lecture organised by Pels Rijcken on 10 December 2020.

[155] The first test phase of the CoronaMelder app also started in the eastern part of the country in July 2020 on the basis of consent.

agreed with this stance. A new section 6d was ultimately added to the Wpg, creating a specific basis for the processing of personal data by the minister and the GGDs with the deployment of the CoronaMelder app.

Effectiveness?

In a position paper on the COVID-19 app, the WRR warns about 'techno optimism': the idea that the introduction of a new technology can, in itself, provide a solution for complex and intractable societal issues.[156] Although few would claim that the CoronaMelder app is *the* way out of the COVID-19 pandemic, there is still little known about the effectiveness of coronavirus apps. The inquiry into the effectiveness of coronavirus apps is also relevant from a privacy-law perspective.

Interference in the personal life of citizens is only permitted if the interference is necessary and proportional. In legal terms, we are talking about the principles of *subsidiarity* and *proportionality*. In other words, the app must contribute effectively to the source and contact investigation, and there may be no less drastic but equally effective means of achieving the objective. The interference must also be reasonably proportionate to the envisioned objectives.[157]

In its DPIA, VWS pointed out the seriousness and effects of the virus, the time and efforts required for analogue source and contact investigation, the limited capacity available for that and the fact that analogue source and contact investigation is not effective for warning people with whom you may well have been in contact but whom you do not know. Based on this, VWS believes that the use of the CoronaMelder app is necessary and proportionate. VWS added to this that the effectiveness of the app would be 'exponentially proportionate' to the number of people who install and activate the app.

Recent figures show that approximately 25% of the Dutch population has downloaded the CoronaMelder app.[158] For a significant contribution to combating the pandemic, an adoption rate of 60% is often cited, although apparently no one

[156] Netherlands Scientific Council for Government Policy, 'Tweede Kamer corona-app — position paper vanuit de WRR' [Lower House coronavirus app — position paper from the WRR], Reader roundtable discussion of the coronavirus app, 22 April 2020.

[157] For every data processing operation, the principles of proportionality and subsidiarity must be satisfied, even if a processing operation is based on consent, see *inter alia* Supreme Court 9 September 2011, ECLI:NL:HR:2011:BQ8097 (Santander).

[158] Factsheet CoronaMelder, 29 December 2020, https://www.coronamelder.nl/media/Factsheet_Corona_latest.pdf.

knows exactly where that percentage comes from.[159] There is reportedly some effectiveness even with a lower percentage (from 15%).[160] Incidentally, it is not entirely clear exactly what is meant by 'effectiveness' in this context, because a definition is lacking and VWS has not formulated any objectives on this point. For a good understanding of the effectiveness of COVID-19 apps, it therefore seems necessary to await the first results of scientific studies.

Conclusion

There was thorough and consistent attention to privacy protection in the development of the CoronaMelder contact-tracing app. This is expressed in, among other things, the technical design of the app and the special statutory basis that was ultimately created for the use of the app. From a privacy-law perspective, therefore, it appears that the CoronaMelder app has established a blueprint for future apps that could support source and contact investigation.

The big question now is whether these kinds of apps are actually effective and what the critical success factors are in this context. The answer to this question is relevant not only from a political perspective but also from a legal perspective. Because a nationwide coronavirus app that does indeed process personal data but does not contribute to combating the virus breaches privacy in an unjustified manner.

Points for attention

- The CoronaMelder app uses various techniques aimed at preventing data from being traced back to persons, but a residual risk of traceability nonetheless remains. For this reason, the CoronaMelder app has been designed and launched *as if* there could be processing of personal data in all phases of the app.

- On neither the national nor the European level is there consensus on the most appropriate basis for the processing of personal data via a COVID-19 app for automated source and contact investigation. A number of European countries opted to use consent as this basis. In the Netherlands, it was ultimately

[159] N. Mouter et al., 'Nederlanders zijn het niet eens over de wenselijkheid van de corona app' [Dutch disagree on desirability of coronavirus app], 8 June 2020, p. 17-18.

[160] Trouw, 'Hoe succesvol is de corona-app?' [How successful is the coronavirus app?], 30 December 2020.

decided, on the advice of the Dutch DPA, to introduce a temporary law in which a special statutory basis was created.

- The creation of the CoronaMelder app shows that potential privacy risks are increasingly the subject of extensive attention in ICT projects. A data protection impact assessment is a good instrument to identify these risks in advance in a structured and thorough manner and is moreover mandatory in certain circumstances on grounds of the GDPR.

9 South Africa's Approach to COVID-19 Data Collection and Contact Tracking

Paula Kotzé

South Africa follows a multi-pronged approach in its digital COVID-19 tracking and reporting response. The COVID-19 Online Resources & News Portal[161] was set up by the National Department of Health (NDoH) to distribute information on COVID-19. The portal (website) provides information on the Government's COVID-19 risk adjusted response strategy and regulations, news updates, vaccine updates, several resources on COVID-19 and key contact details for various institutions. It is supported by a COVID-19 telephone hotline, 'COVIDConnect', as well as the 'COVID Alert South Africa App'. Use of these services is voluntary. In addition, several dashboards based on COVID-19 statistics supplied by the national, provincial and local spheres of government, as well as by national and private COVID-19 testing facilities, are published and updated on a regular basis, mostly once daily, based on COVID-19 test result data.

COVIDConnect

COVIDConnect,[162] launched in May 2020 by the National Department of Health (NDoH),[163] is an official SMS and WhatsApp information and help service and access to laboratory results (via two different mobile phone numbers) launched in July 2020. The use of the service is voluntary. It works on any mobile phone and does not require a user to have a smartphone. Two different phone numbers are used for general information on COVID-19 (including health checks, news, speeches by the President of South Africa, statistics on the number of cases, alert levels, symptoms, treatment, vaccines, etc.) and for obtaining test results. The WhatsApp

[161] https://sacoronavirus.co.za/

[162] https://sacoronavirus.co.za/2020/07/17/health-department-launches-covid-service-portal/

[163] Going live in June 2020

version requires a data connection to run, either through a WiFi or a mobile data network. For users without WhatsApp, the SMS system can be accessed via USSD prompts. Standard USSD charges applies to the SMS version.

Contact tracing is controlled by the users themselves. If a user has tested positive, the user can use COVIDConnect for informing close contacts the user can remember and have contact details for. Telkom SOC Ltd[164] (a state-owned telecommunications company) provides the COVIDConnect service, which validates test results using date of birth and a PIN provided to ensure fidelity of the system. Reports on user experience and actual usage of the system has been sparse, but some exists in the press. In an announcement on 16 July 2020, the Health Ministry hailed the success of the systems, but it also stated that some resistance and reluctance to use of COVIDConnect was reported early on.[165] A month after the official launch of the service, the service had been used by eight million people in South Africa, 2.5-million people had used the self-screening function, and more than 400 million messages had been processed.[166] The public was also reassured that the service would not infringe on their privacy or data, and that one of the reasons for delay "to implement the system was to ensure that it passes the legal muster and adheres to legal prescripts relating to personal information, confidentiality and individual and data privacy".[162] The major shortcoming of the service is that it cannot reach everybody since between 30% and 40% of people in South Africa do not use WhatsApp, and for the both the WhatsApp and SMS there is a barrier if there is no data or airtime on a phone.[166]

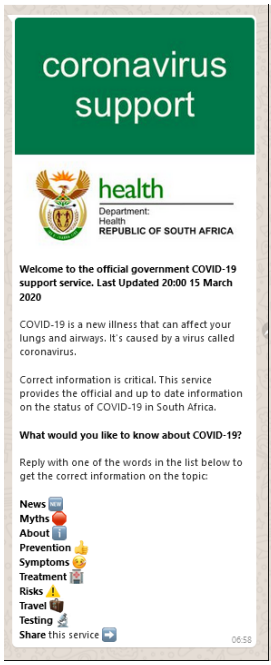
South Africa was the first country in the world to build a WhatsApp channel like this for COVID-19. Two weeks after its launch, the World Health Organisation 'borrowed' the application for global use.[166,167]

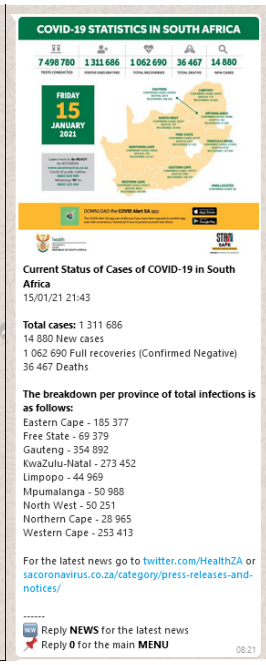
[164] https://www.telkom.co.za/about_us/companyinfo/company-info.shtml

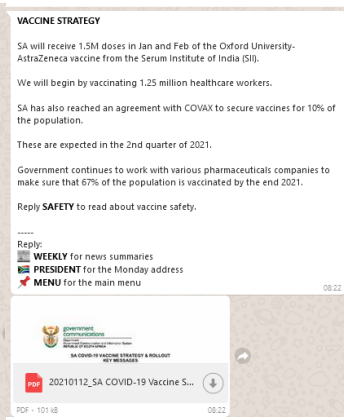
[165] https://www.sanews.gov.za/south-africa/government-launches-covid-19-support-service

[166] https://www.dailymaverick.co.za/article/2020-10-13-covid-alert-sa-app-the-fine-balance-between-public-health-privacy-and-the-power-of-the-people/. The total number of people who have used the system since then, is not publicly available.

[167] https://www.praekelt.org/covid-19-response-in-sa







COVIDConnect Main Menu[168] *COVIDConnect Cases View* *COVIDConnect Vaccines View*

COVID Alert South Africa App

To address some of the shortcomings of manual contact tracing, NDoH decided to build its own contact tracing app, especially to remove the obstacle of having to know or remember close contacts.[166] In August 2020 NDoH launched the *COVID Alert South Africa App,*[169] a free exposure (contact tracing) notification app aimed at notifying users of the app when they have been in close contact with someone who has tested positive for COVID-19. The use of the app is voluntary.

The app, developed by Discovery Limited,[170] one of the largest private medical aid (insurance) providers in South Africa, is operated technically on behalf of NDoH by Discovery Limited, and Telkom SOC Ltd.[164] While the contact tracing is in the user's hand with COVIDConnect, the COVID Alert South Africa App uses technology to enable contact tracing when exposure to a positive COVID-19 person, who has also installed the app, occurs.

[168] Screenshot of COVIDConnect Main Menu

[169] https://sacoronavirus.co.za/covidalert/

[170] https://www.discovery.co.za/corporate/our-business

The app is built on Apple and Google's exposure notification framework.[171,172,173] A notification system based on the framework employs random, rotating keys and identifiers to convey positive diagnoses in addition to data such as associated symptoms, proximity, and duration. The framework defines two user roles, an affected user (with a confirmed or probable diagnosis of COVID-19) and a potentially exposed user (with a current/past proximity to an affected user). Various aspects of the framework can be turned on/off within a specific app developed based on the framework.

Bluetooth

The COVID Alert South Africa App[169] uses Bluetooth signals to exchange 'random codes' (a digital handshake) with other app users when their smartphones are within two metres of each other for a period of more than 15 minutes. The random codes exchanged are stored in a log on each phone for a period of two weeks. If a user tests positive for COVID-19, the user can choose to enter the unique PIN received with his/her test results as well as the user's date of birth (for verification purposes) into the app. When permitted, the app shares random codes stored on the user's phone with a central server.

Other smartphones using the COVID Alert SA App check the central server periodically, throughout the day for random code matches. If a match occurs, the user receives a notification that the device user has had potential exposure to COVID-19 over the prior 14 days (date but not exact time), with advice on what to do next. Because the app does not record any personal information, such as the name of the user, and neither the geolocation of the smartphone when exchanging codes, the app cannot tell the user where the exposure took place, but only the date of the exposure. Data privacy of the app is said to comply with the South African Protection of Personal Information Act, 2013 (Act No. 4 of 2013)[174] in that it collects little personal information, is anonymous and encrypts all information.

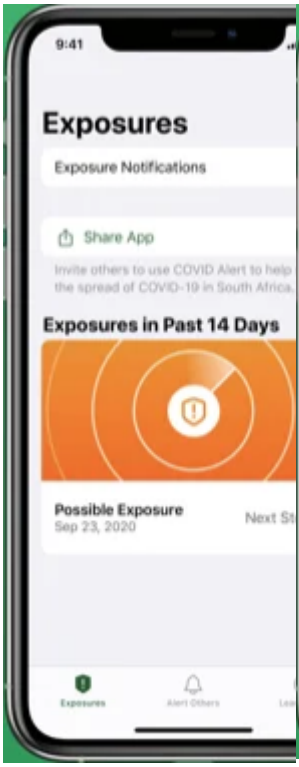
[171] https://covid19-static.cdn-apple.com/applications/covid19/current/static/contact-tracing/pdf/ExposureNotification-FAQv1.2.pdf

[172] https://www.google.com/covid19/exposurenotifications/

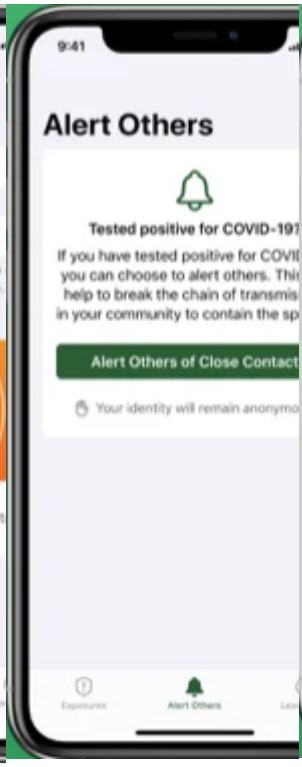
[173] https://developer.apple.com/documentation/exposurenotification

[174] https://www.gov.za/documents/protection-personal-information-act

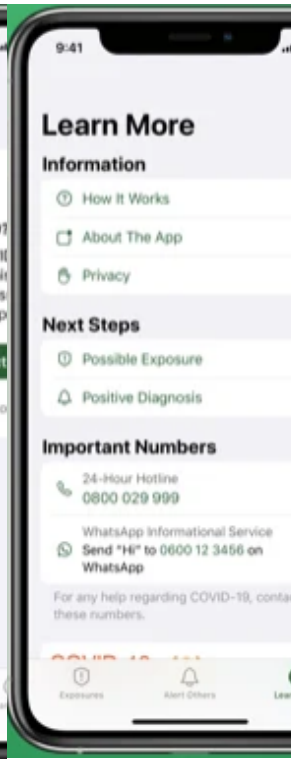
The app is small (latest versions 3.1MB on Android[175] and 8.5MB on iOS)[176] and can be downloaded free of charge, but standard data costs apply when a user downloads the app. The app requires access to a mobile data network or Wi-Fi to run, and although it runs in the background, it requires for Bluetooth and notifications to be enabled all the time. The app is zero-rated (no data costs involved) by all South Africa's mobile network providers. Although the app is touted to work on any Bluetooth-enabled smartphone, it requires Android 6.0 or iOS 13.5 versions to run.[175,176,177]



COVID Alert SA App
Exposure notification[176]



COVID Alert SA App
Alert Contacts[176]



COVID Alert SA App
What to do[176]

[175] https://play.google.com/store/apps/details?id=za.gov.health.covidconnect&hl=en_ZA&gl=US

[176] https://apps.apple.com/za/app/covid-alert-south-africa/id1524618326

[177] https://www.discovery.co.za/corporate/download-covid-alert-sa-app-today

Diverse user experiences

User experience with the app ranges from positive to very negative. Technology issues reported relates to the accuracy of the technology (e.g. signal strength and whether it actually detects other smartphones in close proximity) [175,176,178], the use of the power-hungry Bluetooth radio to be turned on, which results in battery drain on some devices,[175,176,179] the fact that the app does not run on all smartphones in use (older smart phones are still widely in used in South Africa)[175,176] or smartphones that are not compatible with Android and Apple apps[175,176], etc.

Since many South Africans are feeling a bit anti-government due to the whole COVID-19 saga, safety and privacy remains a concern. As a result, some users believe that the app gathers other information from their phones that they have not consented to.[166] Concern is also expressed about the 15 minute exposure timeframe required to trigger as a contact, since evidence exists that an exposure of far less than 15 minutes could result in contracting COVID-19.[175,176] People are also concerned about the delay between exposure and when notification of exposure is received.[175,176] Users of the app who test positive for COVID-19 might only report it several days after they have received their test results. Several users have reported receiving exposure notifications on their phones' notification screens, but when they access the app, no notification appears.[175,176] Also, several users expressed concern that they received a notification for exposure on a certain date, but not where the exposure took place.[175,176] The latter is one of the drawbacks of preserving privacy by not collecting geolocation information.

The app has also received quite positive feedback, ranging from putting the power of technology back into people's hands,[166] to the ease of use of the system and the reassurance in the knowledge that you will be informed if you were in contact with someone who tested positive for COVID-19 (that is if such a person uses and records such information in the app.[175,176]

There have been an excess of 1 million downloads of the app for Android[175], but the number of downloads for iOS is not freely available.[176] How many people

[178] https://theconversation.com/unpacking-the-legal-and-ethical-aspects-of-south-africas-covid-19-track-and-trace-app-147137

[179] https://www.businessinsider.co.za/covid-alert-sa-app-south-africas-official-coronavirus-app-2020-9

actually use the app, is unknown; probably on the low side (in the context of South Africa's estimated population of 59.62 million).[180]

COVID-19 Dashboards

NDoH, health departments of provincial and local governments, the Department of Home Affairs, and the National Health Laboratory Services and private pathology laboratories that perform COVID-19 tests, release regular data on the latest statistics regarding the total number of COVID-19 cases[181] since the first case was identified in the country, the total number of daily cases reported, the number of tests performed, the number of recoveries, the number of deaths specifically attributed to COVID-19 (there could be more COVID-19 deaths that were not specifically indicated as such on death certificates), the number of hospital admissions, et cetera.

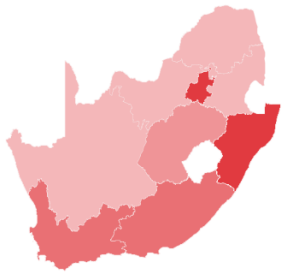
The frequency of the release of this data varies from daily to weekly. This data ends up on various dashboards where the current situation and trends over time are reported. Many institutions and individuals rely on information from these dashboards to keep up to date on what is happening regarding COVID-19 infections in and around the country and in their region.

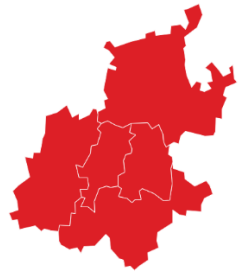
An example of such a dashboard is the one published by a local online news service, News24.com.[182] The dashboard gives a breakdown of cases, etc. down to sub-district level, where such information is provided by provinces to this level.

[180] Mid-year 2020 estimate:
http://www.statssa.gov.za/?p=13453#:~:text=South%20Africa%27s%20mid%20year%20population,%25)%20living%20in%20this%20province.

[181] Individuals who tested positive for the virus

[182] https://covid-19dashboard.news24.com/





TOTAL CASES +1.15% **1 311 686** TOTAL DEATHS +1.72% **36 467** ACTIVE CASES +0.62% **212 529** RECOVERIES +1.23% **1 062 690**

NEW CASES **14 880** NEW DEATHS **615** HOSPITALISATIONS +1.49% **17 147**

TOTAL CASES +1.12% **354 892** TOTAL DEATHS +1.47% **6 819** ACTIVE CASES +1.36% **49 833** RECOVERIES +1.07% **298 240**

NEW CASES **3 916** NEW DEATHS **99** HOSPITALISATIONS +1.10% **5 162**

National testing

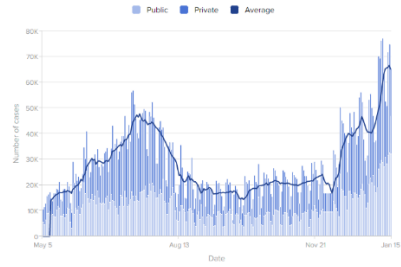
15 January 2021

A total of 7 498 780 coronavirus tests have been conducted to date - 3 163 696 in the public sector and 4 335 084 in the private sector. In the past 24-hours, 31 913 tests were conducted in public laboratories and 33 296 in private laboratories.

7-Day Average: National Daily Tests: Public & Private

For the past seven days an average of 65 014 tests were done every day.

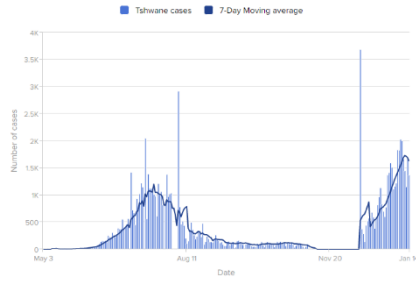
NOTE: Testing data is averaged from 26 November to 2 December because no data was reported.



Daily Cases (7-Day Moving Average)

15 January 2021

Tshwane has reported 1 379 new cases in the past 24-hours, resulting in an average of 1 626 new cases per day for the past seven days.



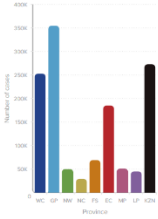
Provincial Comparisons

15 January 2021

On average over the past seven days, Gauteng has recorded the highest number of new Covid-19 cases per day, with a daily average of 4 598 new cases. It is followed by KwaZulu-Natal, which has recorded on average 4 530 new cases in the past seven days.

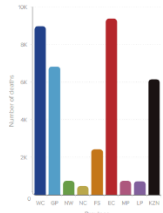
Cases

Gauteng has recorded the highest number of cumulative Covid-19 cases at 354 892 and has an estimated 49 833 active cases. KwaZulu-Natal has recorded the second highest number of cases with 273 452 and KwaZulu-Natal also has the highest number of active cases at 69 650 active cases.



Deaths

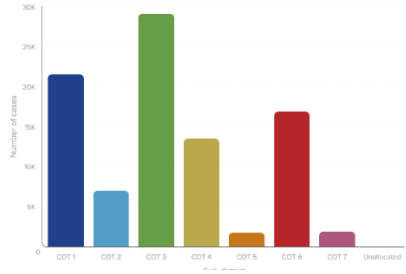
The Eastern Cape has recorded the highest number of Covid-19 deaths with 9 383, followed closely by the Western Cape with 8 965. On average, KwaZulu-Natal has recorded the highest number of deaths per day, at 154 per day for the past seven days, followed by the Western Cape with (on average) 142 deaths per day in the past week.



Cases by Sub-District

15 January 2021

With 29 088 cases the COT 3 sub-district has reported the highest number of cases in the Tshwane district and 24 091 recoveries.



News24.com National Level Examples[182 above]

News24.com District and Sub-district Level Dashboard Examples[182 above]

Conclusions and Insights

- If use can be scaled to most of the population, the value that can be gained by information collected through the *COVIDConnect*[162] app and the *COVID Alert South Africa App*[169] towards the government's initiatives fighting the coronavirus, can be major. Until such penetration is reached, the value will be limited to being an information service to the public on the COVID-19 pandemic.

- Privacy and security concerns are paramount to the use of COVID-19 apps. Mistrust on what the government can do with the information collected, or what other information might be collected without the knowledge of the user, or what other things are installed on the user's mobile phones that they do not know about, are some of the concerns raised and which may hamper the use of the apps.

- The cost of using the apps and the type of device required are both limiting factors in the use of the apps. Although the *COVIDConnect* app could work on any phone (also feature phones and low-end or older smartphones), the cost of use remains a limitation; in the case of the SMS system the USSD cost involved, and in case of the WhatsApp version the required access to a Wi-Fi or mobile data connection. The *COVID Alert South Africa App* requires access to newer smartphones using either Android 6.0 or iOS 13.5 or later. It also requires access to a WiFi or mobile data network for communication with the servers. The use of older smartphones and feature phones are still prolific in South Africa.

- Doubt has been expressed of the value in the delayed notification by the *COVID Alert South Africa App* of a possible contact with COVID-19 positive individual. Doubt has also been expressed in the value of the system if not everyone has the system installed and running (i.e., Bluetooth always on) on their devices.

- The recent saga around the new terms and conditions for WhatsApp may also affect the future of both the *COVIDConnect* app and the *COVID Alert South Africa App*. These changes are currently investigated by South Africa's

Information Regulator.[183] Many users have already left the WhatsApp platform or are planning to do so soon.

- The use of statistical dashboards to convey the extent of the impact of the virus, remains a valuable tool of information to all spheres of government, healthcare providers and the general public. The numbers represented on these dashboards do, however, only represent reported cases of individuals who have tested positive for the virus. The impact of the virus may be much wider, since not all people affected by the virus may have reported for testing.

[183] https://businesstech.co.za/news/technology/460866/south-african-regulator-reviewing-new-whatsapp-policy-changes/

10 Financial aspects of COVID-19 apps

Martin van den Berg and Klaas Brongers

In addition to causing a great deal of human suffering, the COVID-19 pandemic has shown remarkable developments in the digital domain. ICT and data are being used on a large scale as a means of combating the coronavirus and its effects. Personal technology and generic infrastructure enable us to nonetheless continue to do our work and our shopping. The digital transformation of people and society has been given a fantastic boost by the pandemic. Under pressure, a lot becomes fluid; including digitalisation. While in a normal situation, initiatives and projects make their way through decision making and implementation laboriously, urgency prompted innovation and acceleration. One of these projects is the introduction of COVID-19 apps for contact tracing. From an international perspective, many countries built and rolled out this kind of system in a short timeframe. We focus here on the financial angle. ICT costs money, but how much actually?

What is known?

As far as we could find, no comparative investigation has been conducted into the financial aspects of COVID-19 apps. Different types of solutions have been compared with each other, however.[184] We therefore used public online sources. The costs of developing the coronavirus app in the Netherlands were estimated in June 2020 at probably a maximum of €5 million.[185] That gave rise to lengthy discussions on Tweakers of what that amount was spent on.[186] In November 2020, it was reported that another €6.8 million had been earmarked by the cabinet for

[184] https://ieeexplore.ieee.org/abstract/document/9144194

[185] https://www.agconnect.nl/artikel/kosten-nederlandse-corona-app-blijven-onder-de-5-miljoen-euro

[186] https://tweakers.net/nieuws/173308/overheid-gaat-opzet-ontwikkeling-corona-app-wellicht-in-toekomst-vaker-gebruiken.html

the further development of coronavirus apps.[187] The German app will probably cost €69 million. The breakdown is as follows.[188] Development of the German app cost approximately €21 million. Maintenance is budgeted at €45 million. Most of the maintenance costs are for the hotline that people can call if they have questions.

This is an enormous budget compared to Switzerland. There, the costs for developing a similar app only amounted to €1.7 million, and this mobile application could even be rolled out earlier. The Australian app reportedly originally cost AU$2 million, but with all the promotion around the app, it is expected that the cost will rise to AU$70 million, the equivalent to approximately €44 million.[189] Of the AU$70 million, 64 million is expected to go to promotion of the app, with the remainder going to development. In the United Kingdom, the app cost an expected £35 million, the equivalent to approximately €40 million.[190] Of that £35 million, 10 million was spent on the development of an app that was very quickly abandoned because of technical deficiencies. In France, government employees developed the app. Monthly costs of approximately €100,000 are expected.[191] In relation to the United States, it is known that only a few states have made an app available.[192] A list can be found on Wikipedia indicating which countries developed an app, but information on costs is not provided.[193]

In a detailed study of COVID-19 contact-tracing apps, 16 apps were compared to each other from the perspective of architecture.[194] Three types of architecture are distinguished, central, decentral and hybrid architecture, each of which has its advantages and disadvantages. The study provides good insight into aspects such as the expected quality of the diagnosis, the manner of installation, data management, privacy, information security, protocols, vulnerability, distance

187 https://www.security.nl/posting/678206/Kabinet+trekt+6%2C8+miljoen+euro+extra+uit+voor+doorontwikkeling+corona-apps

188 https://www.agconnect.nl/artikel/dit-het-zwarte-gat-van-de-duitse-corona-app

189 https://www.9news.com.au/national/coronavirus-COVIDsafe-app-could-have-cost-contact-tracing-millions-in-advertising-government-health-news/bd69cbbe-ad14-4547-baf9-eb81aead1198

190 https://www.digitalhealth.net/2020/09/timeline-what-happened-to-the-nhs-contact-tracing-app/

191 https://www.ft.com/content/255567d5-b7ec-4fbe-b8a9-833b3a23f665

192 https://eu.usatoday.com/story/tech/2020/12/06/coronavirus-contact-tracing-exposure-apps/3849099001/

193 https://en.wikipedia.org/wiki/COVID-19_apps

194 https://ieeexplore.ieee.org/abstract/document/9144194

determination, use of open source and connection with Apple or Google operating systems. Development, management and implementation costs were not included in the comparative study. In the conclusion, differences in operational costs are reported, but a substantiation is missing. The Dutch coronavirus app is not part of the study.

What stands out?

- Every country, even in Europe, is developing its own COVID-19 contact-tracing app. *In the US, this is even taking place on the level of individual states.* The question is why countries did not join forces and why one app was not developed, possibly in cooperation with one or more suppliers.
- The architectural approach and aspects were carefully investigated and translate into various advantages and disadvantages. The translation into costs is missing, however.
- There is only anecdotal evidence of the costs of the apps. In some countries, such as the United Kingdom and Germany, there was a great deal of discussion about costs and there are a number of websites that published information on this topic. For other countries, such as Belgium, there is nothing to be found. This could mean that the development of the app went according to plan there and that the costs turned out better than expected or remained within budget. We do not know that at this point.
- What is considered included in the costs of an app differs from case to case. From the examples, it emerges that in Germany, the app costs included the costs of a hotline, while in Australia, the costs included the costs of promoting the app. It is certain that all countries had to incur costs to promote their app, but those costs are not attributed to the app itself in those countries. Comparing the costs of COVID-19 apps is like comparing apples to oranges, therefore.
- A careful comparison of the development costs of the app shows significant differences: from €1.7 million in Switzerland to €21 million in Germany and €40 million in the United Kingdom (2 attempts). It should be noted here — as already mentioned above — that it is not known exactly what is considered included in the development costs. The differences are nevertheless substantial. The Netherlands is at the lower end, with a maximum of €5 million.

What does this teach us?

The way in which apps are developed, implemented and managed varies. There is no uniform idea as to what costs should be attributed to the development, implementation and management of an app. In our view, however, it is incorrect to focus only on the costs of the app as such in this context. The point ultimately is the product or service in which the ICT is packaged and what is needed to put and keep that product or service on the market. In this example, it involves a government service for tracing COVID-19 contacts. An app is merely an automated aid in performing source and contact investigation. More is needed than just an app, therefore.

If the app is to be effective, a large percentage of the population must use the app. Time and money must be invested in promoting the app, therefore, as mentioned in the example of Australia. In addition, people are still needed to carry out the contact investigation and to answer questions from app users, like the hotline in Germany. We can imagine that a telephone information service in the Federal Republic of Germany would be a good bit more expensive than in the Netherlands, given the size of the population. It would make more sense to determine the costs of tracing COVID-19 contacts on a per capita basis. This should yield figures that lend themselves better to comparison.

We would have to see these in relation to the importance attached to the tracing service in that case. Countries that attach no importance to this, or where use of such an app is not possible (in view of matters such as the degree of penetration of mobile phones or network coverage), probably have no manual source and contact investigation and, as such, also no app.

In short, we must abandon the notion of total cost of ownership (TCO[195]) for ICT services on their own. Instead, we should move towards a TCO for business services. Performing source and contact investigation is an example of this kind of business service. A service in this sense is a transaction in which a non-physical good is provided. The TCO must include all the costs for implementing and operating such a service, so including marketing, promotion, IT, service, etc. And these costs must be included for the entire life cycle of the service.

[195] TCO is a term introduced by Gartner. TCO denotes the total amount in costs for the acquisition and ownership of a product or service throughout the entire life cycle/usage cycle.

And the government?

As far as we are aware, all initiatives for developing COVID-19 contact-tracing apps have been government initiatives. Experience teaches that the relationship between government organisations and digitalisation is difficult. Insight into the costs of ICT at the government is even trickier. A good development in this respect is that our parliament realises this. Kathalijne Buitenweg, initiator of a Permanent Committee for Digitalisation, talks about a lack of knowledge about digitalisation in the Lower House.[196] The new committee's ambition should, in her view, be to ensure that digital developments are discussed in depth, across the board, and in cohesion with each other.

For Ron Roozendaal, CIO at the Ministry of Health, Welfare and Sport and the person ultimately responsible for what has come to be called the CoronaMelder app, an important lesson can be learned from the switch from "how do I account for myself" to "we are going to do this together". He reports proudly that the working method chosen enabled what may be one of the finest coronavirus apps to be developed at record speed for less than $5 million. Whether and how the Lower House has insight into these costs and what its assessment should be are not addressed.

According to scientists Cokky Hilhorst and Lineke Sneller, insight into the ICT costs at the government is not a luxury, but a necessity.[197] This insight does not require that MPs themselves have knowledge of algorithms, DevOps or Cobol; MPs do have to provide good reports that furnish other MPs with the right information. A valuable recommendation, to which it could be added, in our opinion, that what we should be talking about is the TCO for business services, with ICT as one of the components that incurs costs.

Conclusion

Some investigation into the financial aspects of the development and implementation of the COVID-19 apps shows that good insight into costs is lacking. That applies more broadly, more generally in relation to ICT projects. Given the enormous amounts spent on digitalisation ($3.8 trillion worldwide in 2020,

[196] https://ibestuur.nl/magazine/ibestuur-nummer-37

[197] https://fd.nl/opinie/1370904/goed-toezicht-op-ict-overheid-vergt-veel-beter-inzicht-in-de-kosten-jeb1cahkodS9

according to Gartner[198]), it is actually crazy that we apparently still do not have good models for providing insight into ICT costs and enabling comparison.

In addition, the analysis of the costs of COVID-19 apps makes it clear that most of the costs are not attributable to the ICT development, but to the broader implementation of a service in which ICT is one component. So in fact, we need models to provide insight into the costs of business services so that these can be compared. That is not only useful for gaining insight into tracing services, but also as a form of reporting for our MPs.

A few points

- Every country has its own COVID-19 app.
- Comparing the costs of COVID-19 apps is like comparing apples to oranges.
- Providing insight into ICT costs and enabling a comparison still presents a challenge.

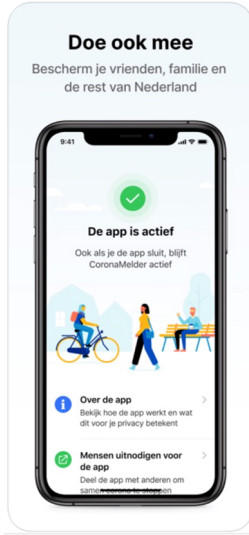
[198] https://www.gartner.com/en/newsroom/press-releases/2020-10-20-gartner-says-worldwide-it-spending-to-grow-4-percent-in-2021

11 Project 2.0: CoronaMelder

Sieuwert van Otterloo

The CoronaMelder is the Dutch contact-tracing app for coronavirus infections that was developed for the central government. In the period of 10 October to the end of 2020, the app was downloaded 4.3 million times and therefore evidently gained the trust of many people. We investigate whether this trust is justified. Did the development of the app devote sufficient attention to reliability and security? The technical development and structure of the app was looked at to answer this. How long did it take to develop the app? What kind of technology is used in the app? How complex is the code, can the app be maintained and how is security provided for?

Technical transparency



The CoronaMelder is an example of a government-led automation project that is striking in two respects. Firstly, it was realised in a short time frame, just a few months. This is exceptional, because many projects take several years. As can be seen on the central government's ICT dashboard,[199] government projects often involve a timeline of years. This was done in a number of short sprints.

Secondly, the result of the project is transparent. The entire code of the project, including design documents, has been published on the Github digital platform. This enables good, objective analysis. This approach is extremely commendable, because without this transparency, no technical analysis would be possible. This is unique within the app store as well: the source code, design documents and security tests are not available for any of the other apps in the app store. All the criticism from a technical angle is therefore

[199] Central government ICT dashboard

relative: The fact that the app is open to analysis and that critical analysis can be performed already distinguishes it positively from other apps and projects.

The CoronaMelder app is never a completely finished product, which is entirely in line with modern principles for app development. Version 1.1.0 was developed on 11 August 2020 and has been updated approximately every two weeks thereafter. The technical analysis is therefore a snapshot at a moment in time.

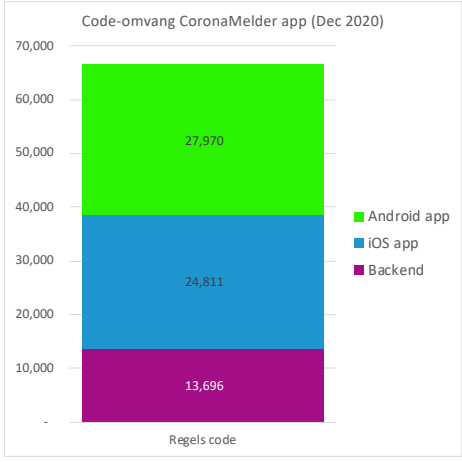
Architecture

According to Van Dale, an app is an application for a smartphone or tablet. Apps can be developed in a number of ways.

- option one is to create apps that work entirely on the smartphone without the help of a central server;
- option two is to create apps whereby some important functions are performed on a central server ('back-end);
- option three is to realise all the functions in the back-end and to only create what is almost an empty shell on the smartphone.

The advantage of the third option is that the app's functionality can be improved at any point by making changes to the back-end. At the same time, this is a disadvantage: the behaviour of the app is determined by the central server and can therefore be changed at any moment.

The CoronaMelder follows option two. The app performs much of the interaction with the user itself (mainly explanation) but exchanges data with a back-end, which tracks the data of all users. To make it extra complex, there are actually two separate apps: one for the iOS platform, used by all Apple phones and tablets, and one for the Android platform, which is used by virtually all non-Apple phones and tablets.



Both apps use the same back-end. The back-end accounts for approximately 20% of the code. This quantity,

expressed in numbers of lines of code, which says something about the maintenance burden, is shown in the graph.

Both apps were developed in two different programming languages: Swift[200] for iOS and Kotlin[201] for Android. These programming languages are the preferred app development languages of Apple and Google, respectively. These are familiar languages to app developers. So there are many developers who can understand this code.

Disadvantage

The main disadvantage of this choice to have separate apps and programming languages is that there is no guarantee that the two apps will do the same thing. You will always have to test and check both apps to be certain that they are both operating identically and correctly. This makes maintenance more difficult and more expensive.

The back-end has been developed in a third programming language, specifically C-sharp.[202] This is a general-purpose programming language developed by Microsoft. It is conspicuous that this means that (all three) major US technology companies (Google, Apple, Microsoft) are represented.

An important basis for the functioning of the app is the GAEN protocol (Google/Apple Exposure Notification protocol[203]). This protocol was developed in mid-2020 by Google and Apple and ensures that Google and Apple phones can communicate that they have been in proximity to each other. Without a common protocol, it would have been extremely difficult to ensure that Android phones and Apple phones would recognise each other.

Development lead time

The app was developed based on a schedule of requirements published on 19 May 2020.[204] The app was therefore developed over a period of three months (until the first version) to six months (launch). The graph below shows the number of code

[200] https://nl.wikipedia.org/wiki/Swift_(programmeertaal)

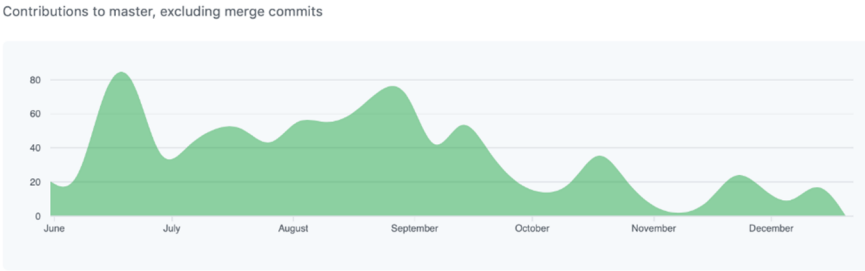
[201] https://nl.wikipedia.org/wiki/Kotlin_(programmeertaal)

[202] https://nl.wikipedia.org/wiki/C♯

[203] https://en.wikipedia.org/wiki/Exposure_Notification

[204] The schedule of requirements for a digital solution for supplementing source and contact investigation, published on 19 May 2020 https://www.rijksoverheid.nl/onderwerpen/coronavirus-app/documenten/publicaties/2020/05/19/programma-van-eisen

additions (commits) in the version management system, from 1 June 2020 to 24 December 2020, for the back-end. Most of the changes were made in the period up to 1 September; the speed of change decreased after that point.



In analysing these data, it is important to know that not all the activities of the development team are visible in the public Github. The development team uses its own version management system and copies their code to the public version management system. After all, it was not the intention that unknown developers could actually work on the app. The 'community' did play a role in contributing ideas for the design and providing feedback, but the app itself was programmed by a team selected by the government. According to people involved, there was a great deal of input from outside this team for the design and testing by means of discussions via Codefor.nl.

Analysis of maintainability of the code

By looking at the code, one can determine whether the system has been developed according to best practices and can consequently be easily maintained. The following stands out.

- Test code. Approximately 70% of the code is normally functioning code and 30% of the code is test code. This is a good result. In code reviews, just 40% of new systems have more than 25% test code. The 30% test code means that many simple errors are found automatically.
- File size. Files smaller than 200 lines of code can be analysed easily. Larger files pose a maintenance risk. 70% of the code is in small files. There are only a handful of files that contain more than 500 lines of code.

- Generated code. A Google protocol buffer routine was used to generate automatic code.[205] You cannot modify the generated code directly, but must modify source files in a language specific for the protocol and generate the code anew. This makes this part of the code more difficult to maintain.

All in all, the code satisfies the standards for code that needs to be easily maintainable. Another team with experience with C-sharp, Swift and Kotlin could maintain and further develop these apps and the back-end itself. This would have to be a multi-person team, because there are multiple technologies.

Despite the fact that the separate files can be easily analysed, it is not easy to read what the lines are if someone is a notification. This is because the GAEN protocol uses all sorts of technical keys that must be sent securely by the app. There is a lot of code in both the apps and the back-end that does not concern things recognisable to the user, but rather technical matters, the packing and unpacking of messages that the apps and back-end exchange with each other.

That is different from most apps, where the code mainly concerns screen elements and functions that are visible for end users. Below are the names of the largest code files from the back-end that relate to technical matters:

Back-end — largest files	**lines of code**
TemporaryExposureKeyExport.cs	331
EksBatchJobMk3Tests.cs	324
TemporaryExposureKey.cs	323
WfToEks_EksBatchJobMk3Tests.cs	314
SignatureInfo.cs	265
TEKSignature.cs	231
IksPollingBatchJobTests.cs	231
ExposureKeySetBatchJobMk3.cs	221
EksEngineTests.cs	212
LoggingExtensionsIccBackend.cs	207

[205] https://developers.google.com/protocol-buffers

Four of the ten files contain only test code (the files that contain 'Test' in the name). Files like TemporaryExposureKey.cs contain code to unravel and validate messages that have been exchanged.

The maintainability for other app developers is good, therefore; the risk of incorrect maintenance is small. This does not mean that the transparency for end users is adequate, however: from the code alone, it cannot be easily seen if the app makes a notification.

Information security

It is important that the CoronaMelder does not any entail any risks in relation to information security. After all, this could cause sensitive health information to be leaked or could — rightly — cause people to be worried. Fortunately, a number of reviews were carried out in August 2020. The outcomes of these are also publicly available:

1. in the report from Radically Open Security, the design of the encryption was analysed, along with the back-end code;[206]
2. the report from Secura looked at both apps;[207]
3. The NFIR performed a penetration test on a number of portals.[208]

All three reports are appendices to a guidance report.[209] Each of the three reports identified a number of points of improvement that had to be fixed.

It is good that a number of security tests were carried out. It is a missed opportunity, however, that these security tests were a one-off: The reports do not mention when a follow-up measurement will be performed and where these results will be available. It is better to systematically repeat these kinds of tests, because the CoronaMelder app changes frequently.

Conclusion

Is in a number of respects, the CoronaMelder app is a positive example for other apps. Firstly, the code is available for external review. In addition, a stable and reliable structure was chosen: well-known, modern programming languages and

[206] Appendix I - Codereview Radically Open Security.pdf — 28 August 2020

[207] Appendix J Secura - Source Code Review CoronaMelder, Android and iOS application

[208] Appendix K - NFIR Report on Penetration Test

[209] https://github.com/minvws/nl-covid19-notification-app-coordination/tree/master/privacy/Duidingsrapportage

best practices were used, which included the following of automatic unit tests. The information security was also reviewed by no fewer than three external companies.

The user functions of the app are not easily verifiable in the source code, however. The CoronaMelder app consists of multiple components in three entirely different programming languages. The code itself has been set up logically but contains many technical details that are evidently necessary in order to use the chosen protocol. The code of the app itself is large but easily readable and equipped with automatic testing. This means the app could be reused for other countries or in the event of another pandemic in the future. A condition for this would be that the security tests performed be repeated on a regular basis in order to permanently safeguard security.

Some considerations

- The CoronaMelder app demonstrates that it is possible, even in a short time frame, to develop a working app with easily maintainable source code. This does require a large team, because many apps involve multiple components, based on complex protocols.

- The app was developed entirely transparently, since the source code is publicly available. This approach should be followed for every government project.

- Publishing the source code alone is not enough to provide users with insight and inspire confidence. This requires additional testing and analysis by experts.

12 (Mis)understanding open-source software

Victor de Pous

COVID-19 apps focus renewed attention on open-source software: a legal model for the development and dissemination of computer programs in which the source code is made freely available. The crux of open-source software is a special licence (category) with broad rights of use at no charge, emphatically in deviation from traditional supply conditions, which are largely restrictive in nature. The choice for open source can be based on various considerations. In the event of digital contact tracing by government organisations, the main reason seems to be to alleviate distrust. Technological transparency means no hidden functionality and thus, in principle, no secret (mass) surveillance. But this objective does not require an open-source licence. There is also sometimes a desire for third parties to help improve the quality of the application. Or the choice for open source may be motivated by a social commitment to make the software available free of charge. If someone supplies software under an open-source licence, they give literally everyone, without discrimination therefore, the right to freely use the code, as well as modify it and pass it on.

Tone set

Governments know what they are doing. Or at least, that is what the use of open-source licences for the development and/or supply of contact-tracing applications for combating the SARS-GoV-2 coronavirus ('COVID-19 apps') and the underlying information system would suggest. A government that wants to secure the voluntary cooperation of the average citizen in an era of rampant fake news, conspiracy theories and sometimes profound political polarisation cannot avoid digital transparency and explanation to eliminate or at least limit distrust.

The proposals submitted on grounds of the appathon[210] organised by the Dutch Ministry of Public Health, Welfare and Sport had no choice therefore but to

[210] See chapter 5.

go public, even though the tender did not explicitly require this.[211] Insight into the sources gives experts the opportunity to assess the software.[212] The central government's promise of transparency evidently translated at the app providers — automatically and indiscriminately — into the publication of their code *under an open-source licence*. Almost all seven final coronavirus app proposals submitted to the central government were offered under the General Public License (GPL) 3.0. That was not necessary. If someone wants to publish the source code of a computer program (or other material), they can do that under statutory copyright with reservation of rights.

Background

The American scientist Richard Stallman came up with the legal concept of 'free software' at the beginning of the 1980s.[213] To put it briefly, this is software code that is available to the general public, free of charge, on the basis of a different licence form, with the source code and broad usage rights, and that remains at all times freely available, even upon the distribution of the modified code. *Im Grunde genommen*, free software is a social movement directed against the established ICT companies, who curtail users' freedom and cause undesirable supplier-dependency with their proprietary runcode-only software.

But it would be almost two decades before this new development and supply model for computer programs took root practically. This is because there was no, or hardly any, popular software available that was offered under a free software licence. Linux gradually brought about a change in that. A broader social movement called 'open-source software' — with its less stringent criteria — subsequently encompassed free software around 2000.[214] That said, the Free Software Foundation of yesteryear still exists, and its proponents have little interest in what they consider the watered-down concept of open-source software.

Quality and transparency

After the failed process around Easter 2020, Minister De Jonge (VWS) subsequently prescribed that the new software code to be developed would indeed have to be

[211] https://www.tenderned.nl/tenderned-tap/aankondigingen/192421;section=1

[212] https://www.rijksoverheid.nl/actueel/nieuws/2020/04/15/ministerie-van-vws

[213] https://en.wikipedia.org/wiki/Free_software. See, *inter alia*, V.A. de Pous, *Open source software*, in *Digitaal recht voor IT Professionals [Digital law for IT Professionals]*, Amsterdam, 2016.

[214] https://opensource.org/

'open source'. In his letter to the Lower House dated 16 July 2020, he pointed to the starting point in the development of the app: 'as much transparency as possible'.[215] This also allows a (public) community of programmers to watch along and contribute; a process that can benefit quality.

Was the choice for the open-source model a deliberate one this time? We are unable to figure out a justification for the licence agreement selected for the CoronaMelder app. Community manager Edo Plantinga told the website Tweakers.net: "One of the key starting points is that the code is open source, with the European Union Public Licence as licence".[216] More specifically: EUPL-1.2.[217] This usage agreement belongs to the subcategory of 'copyleft', which means that the dissemination of code, even the modified code, must always take place under the same conditions. On the other hand, the licence does not have 'viral effect', so that in the event of static or dynamic linking, all the associated software code does not suddenly fall comprehensively under the EUPL-1.2 regime.

More vulnerable?

What proponents of open source usually praise is quality. According to them, open source yields better quality than closed-source software, because the public availability of the source code makes it possible for everyone to read along and, above all, contribute to the programming. Aside from the general observation that the deficit in digital quality is, regardless of legal model, a stubborn, generic and major problem society-wide, it is a difficult discussion. Anything you say about an open-source computer program in the concrete case may be correct but does not have general validity on this ground. If, for instance, there is no *community*, there are few pairs of eyes to check the software. And: commonly-used open-source code can also have drastic (security) defects, which only come to light at a delay.[218]

It is established that an open-source project can best be managed professionally and centrally; regardless of whether that is done by volunteers or in exchange for pay. For the record: software management on the user side must also take place carefully, including the urgent implementation of *patches*. It is still an

[215] https://www.tweedekamer.nl/kamerstukken/brieven_regering/detail/2020Z14096/2020D29955

[216] https://tweakers.net/reviews/7994/2/veilige-en-nuttige-corona-app-kan-dat-open-source.html

[217] https://joinup.ec.europa.eu/collection/eupl/news/understanding-eupl-v12

[218] https://en.wikipedia.org/wiki/Heartbleed

interesting question whether the mere fact *that* a source code[219] is public leads to a heightened security risk. Some think so. "The source code is the architectural blueprint of how the software is built", says Andrew Fife of Israeli company Cycode, after it became known in December 2020 that third parties had accessed Microsoft's source codes via the so-called SolarWinds hack.[220] "If you have the blueprint, it's far easier to engineer attacks."

Dependency on Big Tech

In the German case, we see the government as contracting authority paying for the development (€19 million[221]) and prescribing that the development process must take place under an open-source software licence. On 29 May 2020, the government wrote: "Für die Entwicklung der App ist es ein wichtiger Schritt, dass in dieser Woche eine erste Version der Anwendung auf der Open-Source-Plattform Github veröffentlicht wurde."[222] The Apache 2.0 licence applies to the Corona-Warn-App and related software.[223] These conditions fall in the subcategory of 'permissive', i.e. with minimal contractual restrictions for running, modifying and disseminating the software.

The so-called (Google/Apple) Exposure Notification (GEAN) application programming interface (API), which provides for the exchange of Bluetooth codes in between Android and iOS phones, is not open source, however.[224] Senior lecturer at Nijmegen University Hoepman warned about the incorporation of the contact-tracing technology in Android and iOS. As part of the operating system, users cannot remove this functionality (later), which as a rule is possible with apps. He calls it 'a wolf in sheep's clothing'.[225] Earlier, the National Coordinator for Security and Counterterrorism called attention to the notorious dependency on ICT that makes us vulnerable, even society-wide.[226] What is striking is his broader view,

[219] In the CoronaMelder project, 'everything' was made public, including the architecture, the results of penetration tests and, for example, other security tests.

[220] https://mobile-reuters-com.cdn.ampproject.org/c/s/mobile.reuters.com/article/amp/idUSKBN2951M9

[221] See chapter 11 in this respect.

[222] https://web.archive.org/web/20200529161219/https://www.bundesregierung.de/breg-de/themen/coronavirus/corona-warn-app-1747738

[223] https://github.com/corona-warn-app. The app in Austria (from the Red Cross) also uses this licence.

[224] https://en.wikipedia.org/wiki/Exposure_Notification. Also see chapter 3.

[225] https://blog.xot.nl/2020/04/19/google-apple-contact-tracing-gact-a-wolf-in-sheeps-clothes/

[226] https://www.nctv.nl/documenten/publicaties/2019/6/12/cybersecuritybeeld-nederland-2019

which encompasses more threats than just espionage and crime. The Netherlands is (also) 'dependent on a limited number of providers and countries, which makes us vulnerable to their (changing) intentions,' referring here to the US and China.

Forking

Open-source software means pure digital control for users, also in terms of modifying and redistributing another party's software in line with one's own ideas. That also emerged from the practice in relation to the COVID-19 apps. A number of volunteers in Germany, for instance, modified the official Corona-Warn-App, creating a version that is 'entirely free of dependence on Google'. It is good to realise that this process in principle requires no permission from the German government, but ensues from the open-source model. Since 8 December 2020, the mobile application has been available in F-Droid, an alternative app store.[227]

Google Play Services were deliberately bypassed in the migration. "These Google services intervene deeply in the system and undermine the digital sovereignty of the users. By default, this prevents the use of many Corona apps for people who value privacy and software freedom on their Android devices," according to the Free Software Foundation Europe. The independent 'fork' — a new, modified version (line) of existing software — does indeed use the MicroG framework, but Google's tracking functionality has been removed from it.

Purpose limitation

No hidden functionalities, so in this case, in principle, no (mass) surveillance by the state or covert data processing in any other sense. Insight into the source code has appealing aspects, which are not misplaced for a government organisation in a democratic constitutional state. On the contrary. Vigilance is nonetheless called for. The city state of Singapore convinced its citizens early on in the pandemic to cooperate with the TraceTogether digital contact tracing policy.[228] The means: an explicit statement. 'Any data shared with the Ministry of Health (MOH) will be used for contact tracing persons possibly exposed to COVID-19. Only authorised public officers will be able to use the data.'[229]

They were successful. Around the end of 2020, beginning of 2021, approximately 80% of its residents were participating voluntarily. The app was

[227] https://fsfe.org/news/2020/news-20201208-01.en.html

[228] Based on the OpenTrace protocol that is available under the copyleft GPL-3.0 licence.

[229] https://support.tracetogether.gov.sg/hc/en-sg/articles/360043234694-How-is-my-data-protected-

introduced on 20 March 2020 and the token three months later. On 4 January 2021, the government's true intentions were revealed. At that point, Minister Tan (Home Affairs) informed the parliament that the TraceTogether data could also be used for criminal investigations.[230] A broken promise, followed by an amended privacy statement. Also striking: Singapore did not primarily use the open-source model to benefit transparency or quality. "By open sourcing TraceTogether's source code, the team hopes other organisations and countries can build similar Bluetooth-based contact tracing solution suited to their local context, while enabling interoperability across jurisdictions so we can collectively combat COVID-19 globally."[231]

Conclusions

On the whole, attention for open-source software in digital contact tracing does not unambiguously indicate more insight into and knowledge of this anomalous legal construction. What is also striking are the policy choices that can be distinguished. While the Netherlands was in the second instance aiming for optimal transparency[232] *and* quality improvement by making the ICT project public from the start, Spain[233] had its app developed behind closed doors. For the Singapore government, the argument that the source code could be shared with foreign authorities evidently carried a lot of weight,[234] as did the aspect of interoperability for cross-border efforts. It remains relevant that digital transparency in itself does not fully exclude secret data processing and incidents, as is also evident from the example of Singapore, if the data are used for another purpose. And in the Netherlands, we saw data leaks of test results elsewhere in the chain.

The choice of licence also shows a diverse picture, whereby we wonder whether the features such as 'permissiveness' (a lot of freedom for the user), 'copyleft' and 'viral effect' (stricter in nature) were sufficiently well-known and taken into account. But possible lack of understanding about open-source software — in the perspective of government digital tools for (public) health — is likely to have

[230] https://www.bbc.co.uk/news/world-asia-55541001

[231] https://www.tech.gov.sg/media/technews/six-things-about-opentrace

[232] Major efforts were made to eliminate mistrust on the part of citizens. For instance, before the code was made live in the app, a civil-law notary checked each time that what was published on the Github open-source platform corresponded to what was in the app store. Evidenced by a notarial declaration.

[233] In Spain, the source code of RadarCOVID was not made public as open-source software, under the Mozilla Public License 2.0, until social pressure pushed for this. See chapter 20.

[234] Australia in any event copied the Singaporean OpenTrace protocol.

its revenge when anyone and everyone starts releasing their own version of an application and the authorities find this undesirable. For now, the Apple and Google app stores provide some assistance, with their refusal to include 'metoo' COVID-19 apps. There are other ways to disseminate apps as well, however, as we saw in Germany. Incidentally, this 'fork' seems to be an unexpected but welcome increase in the scope of digital contact tracing.

Points for attention

- Open-source software (ten criteria) with free software embedded therein (four freedoms) uses copyright in a deviating or opposite manner, specifically to make and keep the blueprint for computer programs free. That was novel at the time, and the legal model for development and supply based on this became an unprecedented worldwide success.

- A commissioning party or owner would be wise to first determine the envisioned purposes of the software and then mirror these legally. If someone wants to publish the source code from the viewpoint of technical transparency, they can do that under statutory copyright with reservation of rights. If someone does not want any 'metoo' versions or version lines of their application, they should weigh this against the other special aspects of open source.

- Insight into the source code may well provide insight into what an information system does, but it does not prevent any secret or other unlawful data processing, for example because *organisational* protective measures can fall short, there could be intent or an incident could occur elsewhere in the chain (business process). This calls, first of all, for a preventive, comprehensive audit.

- Open-source code development — from the very start, therefore — by a government organisation can come up against particular issues that do not arise in the business sector, or only to a lesser extent. Take procurement law, for instance, the requirement of effectiveness and efficiency, the standing

practice that the Lower House is informed before society, and the public identity of individual employees involved in programming.[235]

[235] Individual public servants involved in the development process of the CoronaMelder app were apparently threatened. https://ibestuur.nl/magazine/ron-roozendaal-open-ontwikkelen-kan-dus-wel

13 Humanity by design: quality approach for digitalisation

Leon Dohmen, Joan Baaijens and Liesbeth Ruoff-van Welzen

When developing a digital facility, general and widely supported security standards, such as the ISO27001, support the principle of secure by design. This also applies in the design of a coronavirus contact-tracing app ('COVID-19 app'). In order to develop humane apps, however, more is needed than secure by design. We propose the design approach of 'humanity by design'. Based on this, professionals and organisations design and build apps 'as human dignity demands'. Besides respecting and protecting fundamental rights, such as our privacy, and complying with statutory security standards, humanity by design also concerns topics such as autonomy, control over technology, human dignity, justice and power relations. European digital skills and professional standards and, for example, the Ethical code of conduct of IFIP play an important role in safeguarding human dignity.

Technology

In the original approach to secure by design, security tactics and patterns are thought up in advance and then selected for the architecture design. This design services as a guide for the developers and builders.[236] Network and information security do not exist in isolation in this context but constitute an integral component together with all other technical hardware and software components that make a digital facility possible. In this context, we distinguish the following categories and components:[237]

1. infrastructure and networks;
2. computer centres, servers and operating systems;
3. databases, interfaces and middleware;
4. applications and (mobile) devices.

[236] Secure by design — Wikipedia

[237] IT modernisation starts with an analysis of the IT landscape (blogit.nl)

No digital facility can be seen in isolation from the organisational and behavioural aspects of the user, however. Humans, technology and organisation are closely interwoven with each other. We see this in the theory of 'socio-materiality', for instance.[238] This approach explicitly asserts: 'that there is an inherent inseparability between the technical and the social'. This means that an architectural design must take the user's position into account. And therefore necessitates a broader approach and design approach. A digital facility like a coronavirus app must ensure the safeguarding and control of human dignity from the very first design. Secure by design does not take this sufficiently into account. We propose the design approach of humanity by design: professionals and organisations build apps in accordance with the rules 'as human dignity demands'.[239]

A humane architectural design

In order to facilitate an integrated architectural design oriented to humanity by design,[240] we describe a guideline that uses social and ethical themes that focus on respecting and protecting privacy, security, autonomy, control over technology, human dignity, justice and power relations.[241] This guide ensures safeguarding and control based on broadly supported standards frameworks and standards. These are translated into architectural principles for the app to be developed and built. We argue for apps that satisfy the criteria for human dignity[242] to be given a special quality mark (see the figure below).

[238] data-crone-orlikowski-2008a.pdf (dhi.ac.uk)

[239] https://www.vandale.nl/gratis-woordenboek/nederlands/betekenis/menswaardig#.YDIsfNWSnmY

[240] Humanity by design also refers to the central theme of smart humanity of the KNVI

[241] See: Opwaarderen_FINAL.pdf (rathenau.nl, p. 47 and Digitaliseren en verantwoordelijkheid [Digitalising and responsibility] | iBestuur)

[242] The term human dignity refers to the collection of societal and ethical themes mentioned in this article.

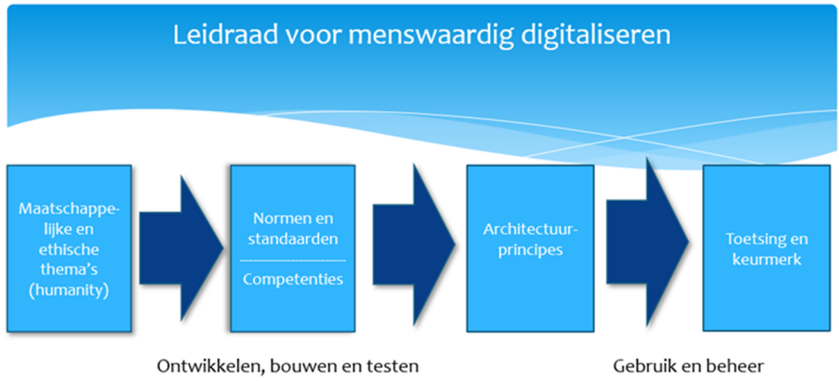


Figure: Guide for human digitalisation (source: KNVI interest group Research and Education ICT; Leon Dohmen, Joan Baaijens, Liesbeth Ruoff-van Welzen)

Norms and standards for network security

For IT security issues, such as network and information security, the ISO27001[243] standard is a generally accepted standards framework. Communication security is a component of ISO27001, which standard specifically addresses network security.[244] Wi-Fi protected Access (WPA2), for instance, is a control mechanism to obtain access to a wireless network. The use of digital certificates and a firewall are other security techniques discussed in this chapter. A Virtual Private Network (VPN) connects geographically separate networks in a secure manner. If someone has access to a network, this does not mean that this person has access to all systems, applications and data within this network.

Specific security themes such as privacy constitute a further detailing of a general move towards secure by design with ISO27001. Design principles such as 'Privacy by Design', based on the General Data Protection Regulation, can tie in nicely with this.[245] Widely supported norms and standards are therefore an

[243] ISO27001 is used as an example here. The standard NEN 7510 could also be read here. This is an Information security standard developed for the healthcare sector in the Netherlands by the Netherlands Standardisation Institute.

[244] Basiskennis informatiebeveiliging op basis van ISO27001 en ISO27002 [Basic information security knowledge based on ISO27001 and ISO27002], by Jule Hintzbergen, Managementboek.nl

[245] Digitaliseren en verantwoordelijkheid [Digitalising and responsibility] | iBestuur

excellent starting point for respecting and protecting fundamental rights such as privacy.

However, ISO27001 devotes little to no attention to behavioural aspects of and relationships between people and the organisational context of which they are part. It is a fundamental part of the distinction between people and technology that people create, experience and change security or insecurity. The technology itself does not do that.

Multidisciplinary competences

Understanding the context and behaviour of people in the use and management of apps such as the COVID-19 app is an under-emphasised competence. This insight is essential in order to prevent vulnerabilities in relation to human dignity during development, building and testing. These processes consist of collaborations of many different experts who work for many different organisations. These experts and their organisations have their own behaviour and organisational characteristics that come together in the development, build and test process. So in addition to the inextricable connection between humans and technology in the use and management of apps, the context of the development, build and test process is at least as complicated.

The standardisation and classification of the behaviour and competences of ICT experts and cooperating organisations is still in its infancy. In Europe, CEN TC 428[246] plays an important role in that. A new business plan (2018) describes that this Technical Committee (TC) is responsible for all aspects of standardisation relating to the ICT profession in all sectors, both public and private. The building blocks of ICT professionalism are: competences, education and certification, ethical code and Body of Knowledge (BoK).

The building block Competences has the first standard EN16234-1: 2019, or e-CF (e-Competence Framework).[247] The e-CF has 41 competences. The e-CF standard also has 'transversal aspects'. This is understood to mean that every ICT professional must be more or less aware of or able to proactively respond in the following areas: accessibility, ethics, legal implications, privacy and security, sustainability and ease of use.

[246] https://www.knvi.nl/kenniscentrum/document/109543/ICT-professionaliteit-de-CEN-Technical-Committee-TC-428

[247] https://www.ecompetences.eu/

Worldwide, first steps are also being taken towards further standardisation in relation to behaviour and organisation. Within IFIP[248], an Ethical Code of Conduct for the professional digital community was recently adopted. The chairpersons of the Committee that set up the code, Gotterbarn and Kreps,[249] assert that an ethical code "does the heavy lifting by offering a well-thought-out guide that well-intentioned people can follow".

The practice

Our point of departure is that humanity by design results in a digital facility whereby humans and technology form an inextricable connection during use and the management phase. In order to arrive at that, a digital facility goes through a design, build and test phase in which norms and standards are essential in order to safeguard human dignity. In the design and build of the software for the coronavirus app, cooperation took place between software and IT professionals and experts in all sorts of domains, such as medical experts and virologists. What that looks like in practice is described in Frankwatching.com.[250] The app must give a warning if there is a risk of infection (function) but must also take all forms of privacy into account. ICT professionals are therefore being asked to do more than just master design methods and programming languages. In order to involve society and organisations in this, more than 180 citizens were spoken with, 979 surveys were administered, more than 750 citizens and experts were taken into account, who proactively provided feedback, and more than 10 UX[251] researchers and designers were on the build team.

This relational connection requires the management of all sorts of collaborative forms to be able to safeguard human dignity in an app. This also involves, for example, the securing of all sorts of information exchange processes between individual professionals in all possible organisational forms. After all, working together also means sharing knowledge and experience of specialist design techniques for linking data files and digital facilities with each other. In order

[248] https://www.ifip.org//

[249] Gotterbarn, D., Kreps, D. Being a data professional: give voice to value in a data driven society AI-ethics (2020). https://doi.org/10.1007/s43681-020-00027-y

[250] https://www.frankwatching.com/archive/2020/10/08/coronamelder-making-of/

[251] A **UX designer** or **user experience designer** is someone engaged in designing a meaningful and pleasant user experience, generally for websites, software programs, apps and games.

to arrive at humane use and management, an overarching organisational policy and joint procedures during the development, build and test process are essential.

Information security policy

A sound information security policy therefore focuses not only on the use and management phase but also on the design, build and test phase. After all, access to and outflow of information, knowledge and experience always takes place via the relationships between the participating organisations and experts who were involved in the development, build and testing of the digital facility. As such, these professionals are always functioning in more or less structured networks of relationships.[252]

The information security policy focused on the development and build networks implies a multi-level management problem. After all, the security management does not only encompass the single developer, the individual expert or the small individual core team of experts. It concerns all cooperating units, in the form of teams, projects and organisations. The 'deeper' management and policy issue in this is who, out of the entire ensemble of partners, fundamentally bears the ultimate responsibility for the result — a humane app.[253] Shared standards and norms, required competences and ethical awareness and behaviour therefore form an essential component for safeguarding human dignity.

Cooperation

The safeguarding of human dignity in the use of a digital facility is therefore strongly influenced by the cooperation, competences and behaviour of experts from the cooperating organisations during the development, build and test phase. The information security policy of the entire system of collaborative relationships, required in order to develop a technically and socially adequate app, then becomes[254] the management of 'joint dependencies'. The development, build and test process always implies the sharing of knowledge and information within a team. Humanity by design refers to standards and values that arise in every form of human interaction. For example, any 'open' and 'free' transaction between

[252] Tasselli, Stefano & Martin Kilduff, Network Agency, *Academy of Management Annals,* 2019

[253] Is it one of the participants who puts himself forward as the party ultimately responsible, or a partner who is designated as such by the others, or is an entirely new — third-party — agency created to bear that ultimate responsibility (transfer of responsibility)?

[254] See, for instance, The Wide Lens, a new strategy for innovation, Ron Adner (Penguin, 2012)

individual people, groups, or organisations requires adherence to certain 'ground rules' (i.e., standards and values) in order to perform the transaction in question. In this sense, ethical standards are also functional to a certain extent in order to enable societal interactions and economic activity and ensure that these take place in a stable manner. These transactions always entail risks, which primarily arise from the individual behaviour of the members ('bounded rationality'). In other words, the security of the whole is formed by the cooperation, competences and behaviour of individuals in combination with the security of the interactions between the collaborating professionals and organisations.

Network and information security

In all of this, during the development, build and test process of an app, the network security professional cannot be seen in isolation from the specific context in which this development takes place. In order to shape the information security policy of this relational development structure, it is necessary to develop an adequate institutional context (legislation and regulations). Both from the strictly data-technical side and from the perspective of substantive-societal aspects (for example: medical, virological, demographics), different social spheres, each with its own legislation, regulation and procedures, are confronted with each other.

Privacy provisions, medical-virological standards and criteria (and economic interests) will have to be connected with each other. Unlocking and combining relevant data sources, in both a technical and institutional sense, is necessary in this context in order to develop digital facilities that respect and protect societal and ethical themes.

Conclusions

The design concept secure by design is too limited in scope, in our view. The inextricable cohesion between technology, humans, society and organisation became visible during the development of the COVID-19 apps. Using norms and standards, a sound information security policy during all phases of a digital facility and using a quality mark would give substance to the new humanity by design concept.

This means the following.

- Respecting and protecting human dignity requires an integrated design approach to technology, organisation and people. Network and information security is a component of this.
- Safeguarding human dignity in use already starts during the design and build process. The common information security policy for different work levels and areas of expertise (individual professional, project team, organisation) therefore encompasses all phases of a digital facility.
- Using widely supported and generally accepted standards frameworks such as ISO 27001 and, for example, NEN 7510 for the healthcare sector, is indispensable in this. Supplemented with norms and standards in relation to competences and ethics. All of this promotes openness and transparency and enables supervision.
- Digital facilities that demonstrably respect the societal and ethical themes deserve a quality mark. This quality mark shows users which apps they can trust when it comes to human dignity and which ones they cannot.

14 The legal status of a coronavirus app under European law

Natascha van Duuren

During a press conference on 7 April 2020, the Rutte III cabinet announced it was considering the introduction of an app in efforts to combat the novel coronavirus. At that point, a contact-tracing app was already operational in China on the mobile platforms Alipay and WeChat. Many countries now have a coronavirus app, including member states of the European Union. This raises the question of the legal status of such an app under European law. In particular, should a coronavirus app or COVID-19 app be considered a medical device in the sense of the law? The answer is of great importance. After all, as soon as it is determined that an app qualifies as a medical device, the rules of the EU Medical Device Regulation (MDR) apply. What does this mean in concrete terms? And what consequences does the upcoming MDR, which takes effect in 26 member states on 26 May 2021, have, and for what parties?

Medical applications

The government — rightly — considers it important that medical devices be safe. Medical devices must therefore satisfy statutory requirements that apply throughout the European Union (EU). Important elements of this include risk classification, (clinical) testing and a mandatory CE mark. This CE mark indicates that the product satisfies the statutory safety and performance requirements. The Inspectorate for Health and Youth Care (IGJ) supervises compliance. Medical devices must satisfy the statutory requirements of the Medical Device Directive 93/42/EEC. Article 1(2) of this directive defines a medical device as 'any instrument, apparatus, appliance, software, material or other article, intended by the manufacturer to be used for human beings for the purpose of investigation, treatment, alleviation or prevention of diseases, injuries or handicaps'. **Medical software (and thus also medical apps)** fall within the definition of a medical device.

Regulation (EU) 2017/145

On 26 May 2021, the Medical Device Directive 93/42/EEC will be repealed and succeeded by the Regulation (EU) 2017/745 (Medical Devices Regulation — MDR). There was a need for rules geared to the cross-border character of innovations. The rules take direct effect in all European Union member states from the moment the Regulation comes into force. The Regulation was already supposed to come into force in 2020, but its effect date was postponed by one year on account of the coronavirus crisis. In and of itself, this is remarkable, because it is precisely now that apps are being developed with the greatest speed in order to combat the coronavirus crisis. It is precisely now that there is a call for (European) regulations to prevent safety risks.

The introduction of the Regulation in 2021 will change the definition of a medical device on a number of points. As a result, medical software that is currently not covered by the current Medical Devices Act will in future indeed be covered by this legislation. The current definition in the Medical Devices Act does not, for instance, talk about *predicting* a disease, while the MDR does.[255] It is precisely this predicting that could be relevant for a coronavirus app.

Manufacturers of software that falls under the definition of a medical device must, from 26 May 2021 onwards, satisfy a number of special requirements, in addition to the rules that apply for medical devices generally. The MDR also has consequences for the risk classification of health apps. The higher the risk a patient runs, the more onerous the check of whether the app satisfies these requirements and may be put on the market. This will put a substantial percentage of the apps in a higher risk category.[256] The risk category of a product also determines who grants the CE mark: the manufacturer itself or (for medical devices from a higher risk category) a notified body.

CoronaMelder

Back to the coronavirus app. Wikipedia describes a coronavirus app as follows: "A COVID-19 app or 'coronavirus app' is a mobile software application designed to automatically register the proximity of other app users. This information can, in the event of a confirmed infection, help to warn people who may have become infected."[257] The definition mentions the 'registration' of the proximity of other app

[255] www.rijksoverheid.nl

[256] www.rijksoverheid.n

[257] www.wikipedia.nl

users, which registration can help us warn people if they have been in the vicinity of an infected person. This ties in with how the CoronaMelder app introduced by the cabinet works:

> **The app sends you a message if you spend some time in the vicinity of a person who is infected with the coronavirus. This enables you to avoid inadvertently transmitting the virus to others.**
>
> 1. The app sees via Bluetooth whether you have been close to someone who also has the app.
> 2. The stronger the signal, the closer you were.
> 3. The app works without your location, name, e-mail address, telephone number or other contact data. The app does not know who you are, who the other person is or where you both are.
> 4. If you have been in the vicinity of someone infected with the coronavirus and who has the app, you will later receive a notification from the app.
> 5. If you contract the coronavirus yourself, you can (voluntarily) indicate this in the app. The app will then warn people with whom you have had contact. **This notification only states when you were in the vicinity of an infected person. It does not say who this person is or where you encountered the person.**[258]

Minister De Jonge (Public Health, Welfare and Sport) decided to introduce a contact-tracing app. In his letter to the Lower House dated 15 April 2020, he expressed this as follows: "The aim of the envisioned tracking and tracing app is to reduce the time between a proven infection and the notification to possible other persons infected by the individual. The GGD will continue to carry out 'regular' contact investigation, and this process serves as a guide. Apps only supplement the process here and are expected to be able to help reduce the time necessary for the investigation and result in more complete insight; a coronavirus app that keeps track of with whom you have had contact and raises the alarm if you have been in the vicinity of someone with a coronavirus infection."

We believe that a contact-tracing app does *not* qualify as a medical device. The (sole) function of the app is, after all, to inform people if they have been in the vicinity of someone infected with the coronavirus. This information says nothing about the actual likelihood of someone being infected with the coronavirus.

[258] www.coronamelder.nl

Incidentally, the position that the CoronaMelder app does qualify as a medical device is indeed defensible. After all, one could take the position that the CoronaMelder app has the aim of detecting possible infections as soon as possible or encouraging users of the app to get tested. Ultimately with the goal of, in the event of a positive test result, taking measures as quickly as possible to prevent further spread and allowing the person who tested positive to seek treatment at an early stage.[259]

De Corona Check app

In contrast to the cabinet, the parties behind the mobile application De Corona Check opted not for a contact-tracing app, but for a medical or health app. De Corona Check app is an initiative of OLVG, LUSCII and a number of partner hospitals spread throughout the Netherlands. The app has been downloaded more than 130,000 times. More than 15 million measurements were sent in and thousands of conversations were held with people.[260] How does this app work? The site reads as follows:

> The De Corona Check app enables you to track your daily health data. Whether you are short of breath or feel like you have a cold. Whether you have a fever and/or a sore throat. And whether you have a cough or have lost your sense of smell or taste. If you have symptoms, the app will advise you to get tested in line with the national policy. You can also request telephone contact with the medical team behind the app. They will then attempt to contact you within 48 hours.

According to De Corona Check, the app is a medical device with a CE mark.[261]

> The data you enter in the app are read out by the medical team of OLVG and the partner hospitals of De Corona Check. This team has been specially set up to provide care in connection with De Corona Check and consists of healthcare providers supported by medical specialists. You may receive an automatically generated message if, based on your answers, you are considered low risk. As soon

[259] See also: Mr. dr. M.C. Ploem & mr. dr. T.F.M. Hooghiemstra, Corona te lijf met een app [Tackling coronavirus with an app], Tijdschrift voor Gezondheidsrecht [Journal for Health Law] 2020(5),), p. 509-523.

[260] https://decoronacheck.nl/over-de-corona-check/

[261] https://decoronacheck.nl/gebruiksvoorwaarden-en-privacystatement

> as telephone contact is necessary, you will always be contacted by employees of the medical team from the partner hospital in your region. Advice via De Corona Check is given based on the information you provide.

This qualification is, in my view, justified. After all, the data entered by the user in the De Corona Check app will be read by a medical team, and this medical team will contact the user if there is reason to do so. Of course it is not ultimately the app that makes the diagnosis. The app is merely conducive in ensuring users are in contact with the healthcare provider on time.

Accelerated introduction of e-health during the coronavirus crisis

On 11 March 2020, the Inspectorate for Health and Youth Care (IGJ) published a news report in which it wrote that the accelerated introduction of e-health could help combat the spread of the coronavirus.[262] It indicated there that in order to guarantee the quality and/or continuity of healthcare during the coronavirus pandemic, it is possible to make a reasoned deviation from existing standards and guidelines. The IGZ stressed that the accelerated introduction of e-health may not pose any threat to patient safety. The use of software without CE mark for diagnosis or treatment is only temporarily possible as long as there are no alternatives available, the healthcare provider can make a plausible case that the application is safe, and necessary care cannot be provided without the use of the application.

Defective compliance with the rules in practice

Although understandable, it is questionable whether it was wise for the IGJ to create the possibility of making reasoned deviations from existing standards and guidelines. After all, these standards and guidelines are there for good reason. In practice, medical device regulations are already being flouted, especially the requirement to ensure a CE mark. It emerged from an investigation report by the RIVM from 2018[263] that of 271 apps investigated, 21% qualified as a medical device.[264] Half of those were missing the necessary CE mark.

---

[262] https://www.igj.nl/actueel/nieuws/2020/03/11/coronavirus-wat-bij-een-tekort-aan-medische-hulpmiddelen

[263] 'Apps under the medical devices regulation'

[264] https://www.rivm.nl/publicaties/apps-under-medical-devices-legislation-apps-onder-medische-hulpmiddelen-wetgeving

Conclusion

The coronavirus crisis has given the market for health apps an enormous boost. The qualification of such apps is of great importance. Apps that fall under the definition of a medical device must comply with the Medical Device Directive. From 26 May 2021, this Directive will be succeeded by the European Medical Device Regulation. The introduction of the Regulation ensures that manufacturers must once again review their health apps. In the growing market for medical apps, the government will have to assume its supervisory role (more) in the context of public health. Users of medical apps must, after all, be able to trust that the application is safe.

The story is different for health apps that do not qualify as a medical device. The safety risks of these apps are less serious, since they are not intended for 'investigating, treating, alleviating or preventing diseases, injuries or handicaps'. Nonetheless, quality and reliability must still be priorities for the use of these apps. After all, the large-scale introduction of tracking and tracing apps whose quality and reliability cannot be guaranteed could be drastic for society.

Concluding remarks

- The number of downloads of all sorts of health apps increased by 600% during the coronavirus crisis.[265] This will undoubtedly have the effect that many commercial parties will develop apps and enter the health market.

- It is important to safeguard the quality and reliability of these apps. It is important to 'separate the wheat from the chaff'.[266] If an app qualifies as a 'medical device', the Medical Devices Regulation (2017/745) provides assistance.

- The European regulation does not seem to apply to contact-tracing apps, such as the Dutch CoronaMelder. Nonetheless, it is important that quality and reliability be guaranteed in the deployment and use of these apps as well. More than 60 scientists from various disciplines sent the cabinet an incendiary

[265] https://www.orcha.co.uk/

[266] This is taking place at, for instance, the National eHealth Living Lab (NeLL) in Leiden. NeLL facilitates scientific research into and validation and testing of eHealth.

letter on 14 April 2020:[267] "The use of tracking and tracing apps and health apps is very far-reaching. Whether we like it or not, these apps will create a precedent for the future use of similar invasive technologies, even after this crisis."[268] Any concessions in relation to quality and reliability could, in my view, create the same precedent, and that is of course what we must guard against.

[267] https://www.uva.nl/content/nieuws/nieuwsberichten/2020/04/kijk-kritisch-naar-nut-en-noodzaak-corona-apps.html

[268] Quote from an interview with Natali Helberger, university lecturer in Law and Digital Technology at UvA and one of the initiators, available at www.uva.nl

15 Digital preparedness of the healthcare sector

Gabriëlle Speijer

Acting under time pressure in a situation in which a great deal is unknown also means risking less optimal choices, on emotional grounds. COVID-19 proved to be an outright accelerator for technology. In the Netherlands, the CoronaMelder was developed, an app that allows you to yourself decide whether your data are made available to the public health authority (GGD), which is responsible for coordinating testing and tracing efforts. How paradoxical this development emerges to be can be seen if we analyse the current healthcare system. Today's technological possibilities are proving quite a challenge to the Hippocratic Oath, which represents the deepest professional values of the physician. There is literally a gap between the world of healthcare as we know it in a hospital, physician's practice or GGD and the one that Big Tech companies would like to project. Getting rid of this parallel universe requires the fundamental step of translating deep professional and societal values into the orchestration of technology and data processing. This can bring us to global healthcare at an entirely different level: data-driven, sustainable, learning and value-based.

Time machine in fast-forward: 2020

The 'appathon', which had nothing of the air of a dusty bureaucratic government project, was supposed to result, in a space of less than two weeks, in two apps to help combat the pandemic.[269] At the same time, the tech giants made a deal[270] to embed Bluetooth-enabled contact tracing capability in the system. In lockdown, with our daily life on 'mute', together we were writing history in fast-forward. From the midst of the crisis, we took steps, supported by the technology world that has been ready to deliver for ages, but what about the recipients?

[269] https://www.rijksoverheid.nl/documenten/mediateksten/2020/04/07/letterlijke-tekst-persconferentie-minister-president-rutte-en-minister-de-jonge-na-afloop-van-crisisberaad-kabinet

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

Digitally prepared?

Globally, we saw that the pandemic forced us to act, under significant time pressure, without clear reliable guidelines based on evidence proved in practice. The challenges faced in taking decisions, [271,272] the demand for reliable insights available at short notice, and models have never been so prevalent.

Various models appeared; for instance, to help policymakers simulate the potential consequences of various measures,[273] to chart out the contribution of digital tracing, [274]based on epidemiological variables, and even combined with the impact of behaviour in the population.[275]

Socio-economic and ethnic differences determine health (SDoH) and therefore infection and mortality rates due to the virus. [276,277] Fine-tuning on the subpopulation level is possible by charting out the heterogeneity of our society, such as a mobility model that provides insight in the short term into the substantial contribution of policy measures. [278] For instance, the tightening of a facemask policy in certain public places, ample availability of (free) testing, and financial support for people who would otherwise be forced to work instead of following quarantine measures can strengthen the lockdown strategy.

The view on a total health situation is missing

From a clinical perspective, the pressure to quickly obtain valuable insights into the COVID-19 virus was at least as great. Symptoms linked to and organs involved in the clinical picture were gradually adjusted, based on new insights from the various disciplines. This exposes how essential insight into the overall health situation is in order to be able to be of added value as a healthcare professional, from every position, in advising, treating and providing guidance. Although technological

[271] https://sloanreview.mit.edu/article/how-to-make-better-decisions-about-coronavirus/

[272] https://gh.bmj.com/content/5/7/e003259

[273] https://www.scientificamerican.com/article/virus-mutations-reveal-how-covid-19-really-spread1/

[274] https://www.ox.ac.uk/news/2020-09-03-new-research-shows-tracing-apps-can-save-lives-all-levels-uptake

[275] https://link.springer.com/article/10.1007/s11023-020-09527-6

[276] https://www.who.int/health-topics/social-determinants-of-health#tab=tab_3

[277] https://www.nejm.org/doi/10.1056/NEJMms2029562?url_ver=Z39.88-2003&rfr_id=ori:rid:crossref.org&rfr_dat=cr_pub%20%200pubmed

[278] https://www.nature.com/articles/s41586-020-2923-3

possibilities are widely available to interpret insights that are continuously digitally connected with each other and collectively contribute to knowledge, it appears that there is still some way to go when it comes to using technology for the benefit of (global) healthcare.[279]

Life-threatening data silos

Interoperability, a description of the exchangeability of information between the different systems, is usually mainly approached technically. In clinical terms, faulty interoperability translates as: in a healthcare process, not being able to access health information, not being able to access this on time or adequately, or not being able to access the correct health information: a serious problem worldwide.[280,281]

Today's healthcare system was literally digitalised during the period when a 'memoir' and writing to one's colleague as a 'paper' one-way street was still commonplace. The healthcare landscape has since developed into countless separate virtual silos, each representing separate clinical practices.

With growing super-specialisation, the average patient receives care at different places, and the lack of interactivity is resolved separately from these digitalised units, for example via e-mails, telephone consultation, apps. This costs healthcare professionals extra time and effort, but more importantly, it often does not contribute to safeguarding that there is one reliable truth for the clinical interpretation of the patient's health situation (in time).

The healthcare information systems that are used in clinical practice are therefore primarily focused on supporting financial administrative processes and to a much lesser extent supporting patient characteristics.[282] Moreover, it appears, despite the stimulus subsidies for online access to patient dossiers [283,284] and the

[279] https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6702215/pdf/41746_2019_Article_158.pdf

[280] https://www.demedischspecialist.nl/onderwerp/details/uitkomsten-peiling-gegevensuitwisseling

[281] https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5565131/

[282] https://www.newyorker.com/magazine/2018/11/12/why-doctors-hate-their-computers

[283] https://open-eerstelijn.nl

[284] https://www.vipp-programma.nl/vipp-centraal/toolbox/2020/infographic-toont-speelveld-rondom-vipp-5

provision concerning electronic copies of patient information,[285] not enough progress has been made in making (all) healthcare information digitally available to the patient in real-time.[286,287]

Confidentiality as basis

Without confidentiality between the patient and healthcare professional, the basis for the (treatment) relationship is missing. From the basis of trust, there is room for vulnerability. Which is crucial in order to accurately get a picture of the health situation together with the patient. Based on the Hippocratic Oath, confidentiality is a fundamental professional value. [288] Aside from the fact that healthcare information can now be found in so many places, despite all the efforts, [289]no one can say with certainty where which information is located.

Moreover, it cannot be (transparently) guaranteed where and by whom healthcare information is used. We can expect today's healthcare director to have skills, knowledge and oversight of the digital developments. In order to constantly guarantee the integrity, privacy and security of healthcare information, the director is therefore also an 'orchestrator'. He or she has a view on the expertise in-house, but also knows when and how to escalate to outside the organisation, at, for instance, the larger and smaller specialist companies, scientific teams and specialised consultants. Unfortunately, we see an extremely recent example of negligence in this area under the responsibility of the GGD.[290]

Freedom to innovate not obligation-free

Managing technology with the inclusion of individualised user experience optimisation based on practice is crucial for proper and safe care.[291] The

[285] https://www.avghelpdeskzorg.nl/documenten/brochures/2020/07/01/vws-factsheet-wet-aanvullende-bepalingen-verwerking-persoonsgegevens-zorg?pk_campaign=nieuwsbrief_07072020&pk_keyword=Wabvpz

[286] https://www.patientenfederatie.nl/downloads/rapporten/352-rapport-digitale-inzage-in-je-medische-gegevens/file

[287] https://www.nytimes.com/2020/03/09/technology/medical-app-patients-data-privacy.html

[288] https://www.knmg.nl/advies-richtlijnen/knmg-publicaties/artseneed.htm

[289] https://www.vzvz.nl/over-het-lsp/hoe-werkt-het-landelijk-schakelpunt

[290] https://www.rtlnieuws.nl/nieuws/nederland/artikel/5210644/handel-gegevens-nederlanders-ggd-systemen-database-coronit-hpzone

[291] https://jamanetwork.com/journals/jama/fullarticle/2676098

development of artificial intelligence without taking into account the values of healthcare and society risks causing extraordinarily harmful consequences, for example from the interest of a limited group with power or profit interests. However logical it may be to have management from the perspective of the doctor, it is perceived as very difficult, to say the least.

Oft-cited motives are vendor lock-in ('preferred partner model'), certification, financing or alleged privacy objections. However, a fundamental approach is appropriate. Fulfilling everyone's role based on responsibility supported by technology, instead of the passive form of accountability that results in an administrative burden, with ultimate steering based on missing expertise.[292] [293] This kind of ecosystem, in which technology is added, replaced, or removed in parts by the healthcare professionals and domain experts (in consultation with the care recipient in question) requires deliberate steps informed by the deep values of society and healthcare.[294]

Learning healthcare system

It is only through awareness that a genuinely digital healthcare will become possible. The importance of *communication* between patient and healthcare provider(s) as the ultimate source of healthcare data deserves much more attention. As soon as communication must yield simultaneously sustainable, confidential, ethical and unambiguous healthcare data freed from the context, however, considerable demands are put on the technology itself and the way in which it is orchestrated.

For example, interpretation within the expert groups requires *flexible connectivity* supported by technology that allows not only the use of international standards, but feeds these seamlessly with knowledge directly from clinical practice. Global availability of reliable (traceable), unambiguously interpretable and valuable healthcare information, also for subsequent generations, and technology orchestration based on responsibility (instead of accountability), from the basis of

[292] https://www.raadrvs.nl/documenten/publicaties/2019/05/14/advies-blijk-van-vertrouwen---anders-verantwoorden-voor-goede-zorg

[293] https://www.zorgvisie.nl/kaljouw-collectieve-zorgdoelen-alleen-bereikbaar-met-doorzettingsmacht/

[294] https://www.scientificamerican.com/article/will-democracy-survive-big-data-and-artificial-intelligence/

each person's field and expertise, with broad, multidisciplinary, flexible teams can put in motion a (globally) learning system.[295] [296]

Conclusion

Society, and in particular our healthcare system, is dealing with an acceleration in the use of technology driven by the COVID-19 pandemic. While most technological capabilities, and many promising ones, have been 'waiting' outside of clinical practices, they appeared good enough, without too much consideration, to serve as a remedy during the crisis, even for the citizen receiving care. The CoronaMelder app, launched via a much-talked-about process, painfully shows how much progress still needs to be made in the rest of the healthcare landscape in terms of digital maturity, data-drivenness, and, above all, necessary management from the heart of the healthcare system.

Broadly speaking, there is a largely passive digitalised healthcare landscape, in which technology is usually considered a 'finished' product that can be taken into use; based on the consumer 'user' perspective. This mindset is now dated and upholds a route that brings with it potentially big risks of expanding the interests of a minority with, for example, an exclusively financial or polarising interest. For safe and good care, it is crucial to take the first step: translating the values of healthcare and society in the orchestration of information and technology principles. An ecosystem that is designed in such a way that everyone's expertise, skills and knowledge contributes sustainably [297] will simultaneously require new business models,[298] so that data will flow as a return for global health. Cooperation, mindset and those orchestration principles can yield an unprecedented breakthrough for healthcare.

Points for attention

- In today's healthcare landscape, which has largely become virtual, the fundamental and structural safeguarding of its deepest values is missing. The Hippocratic Oath and the broader societal values emerge not to have been translated into the principles for information and technology, and that is

[295] https://www.nictiz.nl/wp-content/uploads/ICThealth_nr4_2020_HR_64-65-3.pdf

[296] https://aapm.onlinelibrary.wiley.com/doi/10.1002/mp.13140

[297] https://www.euro.who.int/__data/assets/pdf_file/0008/345797/HEN51.pdf

[298] https://www.iftf.org/uploads/media/SR-1038_Rethinking_Business_Models_01.pdf

indeed what we, as citizens needing healthcare, count on in the professional relationship with the physician.

- *Freedom to innovate and confidentiality* are crucial not only to provide safe, state-of-the art or innovative healthcare, but to be able to provide that necessary direction to the rapid developments occurring now in the growing healthcare landscape (even outside the regular clinical practice). The fact that the input from the heart of healthcare is so indispensable in that context will be evident from the data-driven doctor skills, such as specification of technology, optimisation of user experience and communication (data curation) and cooperation across divergent disciplines. New business models will support this, based on, among other things, the principles of value-based healthcare.[299,300]

- A conscious approach in orchestrating technology is necessary to be able to (continue to) guarantee individual freedom, since value creation in the cyber-physical systems will follow the direction of their underlying orchestration principles. The fact that technology will never accelerate without direction is evidenced by initially seemingly innocent social media like Instagram and Facebook. The responsibility we bear as society for the development of technology is not without obligation, therefore. Leadership is required in every position: as physician, policymaker, director, ICT provider, UX designer, scientist, lawyer, etc.

[299] https://www.vbhc.nl/wp-content/uploads/MasterDoc_Xmas-2020_final.pdf

[300] https://jamanetwork.com/journals/jama/article-abstract/206039

16 The Australian COVID-19 Tracing App Experience

Anthony Wong

A large number of COVID contact tracing apps have been developed during the past 12 months. Digital technologies and contact tracing apps can play critical roles in infection control responses to COVID-19, and in limiting contagion and 'flattening the curve'. Technology, security and privacy, civil liberties and health have come into greater focus during COVID-19. Will improvements in safeguards and privacy inspire public trust and confidence in the uptake of COVID tracing technologies to improve front-line responses to COVID-19? As demonstrated by the Australian experience, there are no absolutes. While digital technology improves the efficiency of contact tracing, it is not necessarily a panacea without public trust and confidence in the legal, societal and human constructs.[301]

Biosecurity Declaration 2020

On 18 March 2020 in response to the COVID-19 outbreak, the '*Biosecurity (Human Biosecurity Emergency) (Human Coronavirus with Pandemic Potential) Declaration 2020* was made under the *Biosecurity Act 2015*'[302] to protect the health and safety of the public. The *Biosecurity Act* recognizes the federal nature of government in Australia with the states and territories having responsibility for the protection of public health within their jurisdiction under their respective public health legislation.[303]

[301] This chapter is for general reference purposes only. It does not constitute legal or professional advice. It is general comment only. Before making any decision or taking any action you should consult your legal or professional advisers to ascertain how the regulatory system applies to your particular circumstances.

[302] *Biosecurity Act 2015* (Cth) s 475.

[303] Refer to Table 1 for the relevant Directions and Orders in each State or Territory.

On 26 April 2020, Australia, a country of about 25 million people, was one of the first countries to release a proximity COVID App[304] to support State and Territory health authorities in Contact Tracing.[305] The use of the COVIDSafe App is not mandatory and uses Bluetooth signals to record encrypted data about close contacts (including a unique contact *identifier*, Bluetooth signal strength and the date and time of the handshake) with other users.[306] The App does not use GPS or any other location-tracking system. Collected data on the device is automatically deleted after 21 days.

If a user tests positive for COVID-19, a health professional will contact the user and seek their consent to upload the encrypted information on their device to the National COVIDSafe Data Store.[307] The Data Store is to be held in Australia, and it is an offence for the data to be retained or sent overseas.

Privacy and Security

The Australian Privacy Act 1988 ('Privacy Act') was specifically amended[308] to protect data in the COVIDSafe App and the National COVIDSafe Data Store, to provide stronger protections for COVIDSafe users and to encourage public acceptance and uptake of the COVIDSafe App. The State and Territory health authorities are responsible for contact tracing and ensuring that COVID app data[309] is used only to the extent required for the purpose of contact tracing. In a leap for constitutional power sharing, the Privacy Act was amended to apply to a State or Territory health authority, to the extent that the authority deals with, or the activities of the authority relate to, COVID app data.[310] The State and Territory health

[304] Department of Health, COVIDSafe app, www.health.gov.au/resources/apps-and-tools/covidsafe-app%E3, accessed 1 February 2021.

[305] Refer to *Privacy Act 1988* s 94D(6) for the definition of Contact Tracing.

[306] Technology behind COVIDSafe, https://covidsafe.gov.au/technology.html, accessed 21 January 2021.

[307] National COVIDSafe Data Store means the database administered by or on behalf of the Commonwealth for the purpose of contact tracing, *Privacy Act 1988* s 6(1).

[308] *Privacy Amendment (Public Health Contact Information) Act 2020* introducing Part VIIIA of the *Privacy Act 1988* (Privacy Act).

[309] Refer to *Privacy Act 1988* s 94D(5) for the definition of COVID app data.

[310] Privacy Act 1988 s 94X(1).

authorities (except Western Australia and South Australia) are also governed by their respective privacy legislation.[311]

Information that State and Territory health authorities collect by any other method (i.e. not COVID app data) is not subject to the Privacy Act. The Australian Federal Government has entered into bilateral agreements with each state and territory health authority to guide the collection, use and disclosure of data from the COVIDSafe App.[312]

It is an offence under the Australian Privacy Act to collect, use or disclose COVID app data for a purpose that is not related to contact tracing.[313] The Singapore government has admitted that its TraceTogether app data can be used "for the purpose of criminal investigation", despite earlier privacy assurances.[314] Singapore has subsequently passed new laws limiting the scenarios in which law enforcement agencies can access the data to investigate serious criminal offences.[315]

A safeguard in the Australian Privacy Act, was introduced to cancel the effect of any contradictory law that could be used to access the data.[316] Interestingly, the COVIDSafe amendments to the Privacy Act have foreshadowed future uses of the

---

[311] *Privacy and Personal Information Protection Act 1998 (NSW), Privacy and Data Protection Act 2014 (Vic), Personal Information Protection Act 2004 (Tas), Information Privacy Act 2014 (ACT), Information Act (NT), Information Privacy Act 2009 (Qld)*. Western Australia and South Australia do not have specific privacy legislation. Administrative instruction, PCO12 – Information privacy Principles Instruction applies in South Australia. Specific health records legislation also applies in Victoria (*Health Records Act 2001*), NSW (*Health Records and Information Privacy Act 2002*) and ACT (*Health Records (Privacy and Access*) Act 1997). Refer to www.oaic.gov.au/privacy/privacy-in-your-state/ for further information pertaining to privacy laws in each state and territory.

[312] Bilateral agreements on collection, use and disclosure of COVIDSafe data, www.health.gov.au/resources/publications/bilateral-agreements-on-collection-use-and-disclosure-of-covidsafe-data, accessed 25 January 2021.

[313] Refer to *Privacy Act 1988* s 94D(2) for descriptions on the permitted purposes. *P*enalty for infringement: 5 years imprisonment or $66,600, or both.

[314] Singapore reveals Covid privacy data available to police, https://www.bbc.com/news/world-asia-55541001, accessed 31 January 2021.

[315] Limits imposed on use of contact tracing data by police, www.straitstimes.com/singapore/limits-imposed-on-use-of-contact-tracing-data-by-police, accessed 3 February 2021.

[316] Privacy Act 1988 s 94ZD(1).

COVID app data, as the above safeguard could be overridden by future laws which expressly permits and provides for access to the data.[317]

The Privacy Act has designated, presumably to remove any ambiguity, that COVID app data relating to an individual is personal information.[318] However, it was surprising to note that the Privacy Act has designated COVID app data as "the property of the Commonwealth, and remains the property of the Commonwealth even after it is disclosed to, or used by a State or Territory health authority or any other person or body". This is a particularly sensitive subject that needs to be reconciled with our current understanding of the rights of data subjects and the tenets of property law.[319]

COVIDSafe App

By 30 September 2020, a total AUD$5.24 million had been spent on development, professional services and operational costs.[320] The Australian Select Committee on COVID-19, reported "that a proportion of the AUD$64 million advertising spend under the government's CovidSafe Strategy was also allocated to promoting take-up of the app in addition to the AUD$5.24 million in development and operational costs."[321] As of 24 August 2020, the number of COVIDSafe registrations had reached about seven million, short of the 40 percent (10 million) registrations that the government had been aiming for.[322] The available evidence suggests that high uptake is necessary for the proximity app to be effective.

The results of a survey conducted by Bond University revealed that the "reason given for not downloading the app included privacy (25%) and technical concerns (24%). Other reasons included a belief that social distancing was sufficient

[317] Ibid s 94ZD(2).

[318] Ibid s 94Q.

[319] For an overview on data ownership, refer to Wong, Anthony,: Big Data Fuels Digital Disruption and Innovation, But Who Owns Data? In: Chaikin, David., Coshott, Derwent. (eds.) Digital Disruption Impact of Business Models, Regulation & Financial Crime ch 2, Australian Scholarly Publishing, Australia (2017).

[320] Mr Brugeaud, Chief Executive Officer, DTA, Senate Community Affairs Legislation Committee Hansard, 29 October 2020, p. 94.

[321] Australian Select Committee on COVID-19, First interim report, December 2020, paragraph 3.66.

[322] Ibid paragraph 3.65.

and the app is unnecessary (16%), distrust in the Government (11%), and apathy (11%)."[323]

A number of stakeholders have raised concerns about the usefulness and effectiveness of the COVIDSafe App as the rate of novel contacts identified has been low. By 26 October, the App had identified only 17 close contacts with COVID-19 who would not have otherwise been captured by manual contact tracing.[324] The South Australian Police Commissioner has indicated that the COVIDSafe App has not been of 'material benefit' to local health authorities.[325]

The Australian Select Committee on COVID-19 has also been critical of the COVIDSafe App and concluded in its December 2020 report that the App has significantly under-delivered, experienced issues with its performance and has been of limited effectiveness in its primary function of contact-tracing to enable an opening up of the economy in a COVID safe manner. [326] The state of Victoria in its parliament inquiry, found that "the effectiveness of the COVIDSafe App for Victoria's contact tracing efforts was insignificant."[327] The inquiry also highlighted the shortcomings of the Victorian contact tracing system at the height of the Victorian COVID outbreak as the system was "made up of components supplied from several companies which were not fully integrated into one end-to-end system."[328]

The National Contact Review[329] recommended that the functionality of the COVIDSafe app should be enhanced for the Federal Government to work with the states and territories to optimise incorporation of COVIDSafe contact information

[323] Institute for Evidence-Based Healthcare, Bond University, Australia, More than privacy: Australians' concerns and misconceptions about the COVIDSafe, www.medrxiv.org/content/10.1101/2020.06.09.20126110v2.full-text, accessed 31 January 2021.

[324] Australian Select Committee on COVID-19, First interim report, December 2020, paragraph 3.68.

[325] COVIDSafe app of no 'material benefit' to coronavirus contact tracing, SA Police chief says, www.abc.net.au/news/2020-11-04/coronavirus-covidsafe-app-effectiveness-questioned-by-sa-police/12846556, accessed 31 January 2021.

[326] Australian Select Committee on COVID-19, First interim report, December 2020, Interim finding 3.2.

[327] Parliament of Victoria, Legislative Council, Legal and Social Issues Committee, Inquiry into the Victorian Government's COVID–19 contact tracing system and testing regime, December 2020, page 11.

[328] Ibid page 85.

[329] The National Contact Review, A report for Australia's National Cabinet, 13 November 2020, www.health.gov.au/resources/publications/national-contact-tracing-review, accessed 2 February 2021.

early in the contact tracing process and on the best means to report usage of the app in contact tracing.

At the time of writing, the Health Minister is due to report on the first 6 months operation and effectiveness of COVIDSafe and the National COVIDSafe Data Store.[330] The Australian Information and Privacy Commissioner has reported that 11 enquiries have been received seeking information or expressing general concern about COVIDSafe.[331]

Check-in Systems

As COVID-19 restrictions are eased around Australia, in addition to the federal COVIDSafe App, the States and Territories have issued directions and orders[332], mandating the collection of contact details of attendees as a condition of selected venues (e.g. hospitality venues, gyms and workplaces) reopening. The contact details are required to boost contact tracing efforts. This has led to a proliferation of check-in systems[333] with different rules applying in each of the Australian states and territories. Many venue operators have outsourced their check-in registrations leading to growing concerns in relation to safeguards pertaining to the collection, storage, use and disclosure of the personal information collected by check-in systems.[334]

Some operators of check-in systems have used the contact details as an opportunity to build up their mailing list to complement their marketing and promotional activities. We are seeing a trend, whereby the states and territories are moving away from the patchwork of private third-party check-in systems and paper-based recording by deploying their own check-in apps within their jurisdiction, and in the case of New South Wales, mandating the use of their QR

---

[330] As prescribed by the *Privacy Act 1988* s 94ZA(1).

[331] www.oaic.gov.au/updates/covid-19-advice-and-guidance/covidsafe-report-may-nov-2020, accessed 25 January 2021.

[332] Refer to Table 1 under Directions and Orders.

[333] The proliferation of QR code check-ins is a 'dog's breakfast'. Is there a better way? - ABC News www.abc.net.au/news/science/2020-11-20/covid-19-coronavirus-why-so-many-qr-code-check-in-systems/12895678, accessed 25 January 2021.

[334] https://indaily.com.au/news/2021/01/06/law-society-warning-over-covid-qr-check-in-data-privacy/; NSW's new mandatory QR codes cause confusion after one day, www.abc.net.au/news/2020-11-24/nsw-new-mandatory-qr-codes-consumers/12912158, accessed 25 January 2021.

electronic check-in systems. A fully electronic digital check-in systems greatly speeds up the contact tracing process. The specifics of the COVID check-in apps in the states and territories vary and a summary is as outlined below in Table 1.

Summary of States and Territories Check-In Systems (as at 30 January 2021)

States and Territories in Australia	New South Wales	Australian Capital Territory	Queensland	Victoria	South Australia	Western Australia	Northern Territory	Tasmania
COVID Check-In System Required for selected venues	Yes	Yes	Yes	Yes	Yes	Yes.	Yes	Yes
App Name	COVID Safe Check-in with the Service NSW app	Check In CBR app	No State App, method for collecting and storing contact tracing information, decision for venue	Service Victoria app	COVID SAfe CheckIn with mySA GOV app	SafeWA app	Territory check-in app	Check in TAS app
Mandatory or Optional	Mandated the use of electronic check-in using Safe Check-in or Service NSW check-in URL webform	Use of the Check In CBR app is optional, contact details may be provided by other means	Must collect and store all records electronically	Use of the Service Victoria app is optional, electronic record keeping recommended	Use of the COVID SAfe CheckIn app is mandatory, if no smartphones use of paper recording log template	Use of SafeWA is optional, method for collecting and storing contact tracing information, decision for venue	Use of Territory check-in app is optional; contact details may be provided by other means	Use of the Check in TAS ap is optional, contact details may be provided by other means
QR Code	Yes, must use government QR code	Yes	Yes, QR code is voluntary	Yes, use of government QR code couraged	Yes, must use government QR code	Yes	Yes, must use government QR code	Yes, QR code is voluntary
Information Collected	Full name, phone number (and email address where possible), date and time of entry (and time of exit where possible)	First name, phone number, date and time of venue attendance	Full name, phone number, email address (residential address if unavailable), date and time period of patronage	First name, contact phone number, premises attended, date and time of visit	Name, phone number and date and time of visit[335]	Name, phone number, date and arrival time	Full name, phone number, and email address	Name, phone number and date and time of entry
Data Retention & Deletion requirements	28 days	28 days	minimum of 30 days and a maximum of 56 days	28 days	28 days	28 days	28 days	28 days
Direction and Order	Public Health Orders and restrictions - COVID-19 (Coronavirus) (nsw.gov.au)	ACT Public Health Directions - COVID-19	Restrictions on Businesses, Activities and Undertakings Direction (No. 12) | Queensland Health	Department of Health and Human Services Victoria | Victoria's restriction levels (dhhs.vic.gov.au)	Public activities | SA.GOV.AU: COVID-19 (covid-19.sa.gov.au)	COVID-19 coronavirus: State of Emergency Declarations (www.wa.gov.au)	Chief Health Officer Directions | Coronavirus (COVID-19) (nt.gov.au)	Resources | Coronavirus disease (COVID-19)
Guidance website	www.nsw.gov.au/covid-19/covid-safe/customer-record-keeping/obligations	www.covid19.act.gov.au/business-and-work/check-in-cbr	www.covid19.qld.gov.au/government-actions/covid-safe-businesses/information-privacy	www.coronavirus.vic.gov.au/record-keeping-contact-tracing-information-business	www.covid-19.sa.gov.au/business-and-work/covid-safe-check-in	www.wa.gov.au/organisation/covid-communications/covid-19-coronavirus-contact-registers	https://coronavirus.nt.gov.au/stay-safe/check-in-app	https://www.health.tas.gov.au/covid19/check_in_tas

Table 1

[335] *Emergency Management (Public Activities No 18) (COVID-19) Direction 2021* Schedule 3(4)(b) prohibits use of contact details for non-contract tracing purposes.

When the Privacy Act was extended to the private sector in 2000, it exempted small businesses (with an annual turnover of less than $3 million with some exceptions)[336] from compliance with the Privacy Act in recognition of the compliance costs for certain small businesses, which were then considered to pose little or no risk to the privacy of individuals.[337]

The introduction of COVID check-in systems have ignited debates as to whether the small business exemption should be removed, as technology has changed the way that small businesses operate. Small business collecting COVID check-in data could potentially misuse the data and be outside the ambit of the current Privacy Act. A review of the Privacy Act is currently underway at the time of the writing as to whether the Australian privacy law is still fit for purpose.

Key Takeaways

- Technology, security and privacy, civil liberties and health have come into greater focus during COVID-19.
- Digital technologies are being deployed in innovative ways to improve front-line responses to COVID-19.
- Despite amendments to privacy laws to cover the use of the COVID app, uptake of the COVIDSafe App is below expectation.
- The COVIDSafe App is more sophisticated than the check-in systems introduced by the states and territories, but the App appears to have taken a backseat in the battle with COVID-19.
- Striking the delicate balance between privacy and public safety remains tricky and challenging.
- Better integration between the different components of COVID tracing systems and management would enhance effectiveness, efficiencies and provide better outcomes.
- Better coordination, uniform and national wide approaches will improve Australia's overall COVID-19 defence capability.
- The government's overall track record on technology deployments requires further improvements and assurances.

[336] *Privacy Act 1988* ss 6D(4)(b)-(f), 6E(1A)-(1D), 6D(9); *Privacy Act Regulation* 2013 (Cth) s7.

[337] Commonwealth, Parliamentary Debates, House of Representatives, 12 April 2000, 15749 (Daryl Williams, Attorney-General)

- Inspiring public trust and confidence in technology deployments including the COVIDSafe App are essential, as technology can dramatically improve the efficiency of contact tracing but not necessarily a panacea–as it will not replace (at least not yet) the need for contact tracers and expert health oversight.

17 European cooperation: cross-border data processing

Dirk de Wit

It seems an eternity ago. In September 2011, this author misjudged a bend during a descent in the Dolomites. The result: a fall and two dislocated fingers. The hand was examined at the medical centre. The x-ray made was then saved to a DVD and given to the patient to show to the specialist at his hospital in the Netherlands. You could call it data exchange, old school. The specialist viewed the images. No new photo was required, and the treatment could go ahead. Practical, simple and without the fuss of interoperability between automated data processing systems of different makes. For the European Union, interoperability had already been on the agenda at that point for a good number of years; specifically to facilitate good and efficient care. To put it briefly, this concerns recording and sharing information 'across institutions', as occurs between healthcare professionals.

Where do we stand today?

We focus on a special form of mutual data exchange. The infectious disease COVID-19 accelerated digitalisation in healthcare in many areas;[338] take online consultations, for instance, and the exchange of images via the Corona Portal for the purposes of nationwide patient distribution. The first wave of coronavirus proved a springboard for app development. The OLVG app, which enabled people to be diagnosed remotely, became very well known very quickly. But the contact-tracing apps ('COVID-19 apps'), which were soon the focus of attention throughout Europe, received much warmer interest, albeit because of the urgency with which this mobile application had to be put into use. We see an acceleration in a form of data sharing in the European context. Before we get to that, we will start at the topic of interoperability in the European perspective. We will then look at the COVID-19 apps. Every ground for exchange starts with the patient.

338 Deloitte, Shaping-the-future-of-European-healthcare, September 2020.

Patient journey

Many health issues can be taken care of with a visit to the general practitioner. Additional laboratory testing, visits to paramedics and a prescription for the pharmacy are common next steps. For some patients, other steps beyond this are needed. The lab results could be followed by a referral to hospital, possible surgery, further referral for rehabilitation or forms of community care. In these cases, the data must travel with the patient, and this takes place increasingly digitally these days. In practice, we are already coming up against difficulties in the Netherlands. Data that are difficult to transfer between systems, different use of concepts, lack of clarity about consent, to name just a few factors. The patient's journey and the data exchange do not necessarily have a digital counterpart. Both nationally and in the European context, the electronic journey of the patient is a major issue in which progress is only being made piecemeal.

Interoperability and network

Data exchange across institutions or across sectors has been fashionably dubbed interoperability. Nictiz describes interoperability as the possibility for different autonomous, heterogeneous units, systems, parties, organisations or individuals to work, communicate and exchange information with each other.[339] How can we connect systems with each other in such a way that data can be transferred electronically without a hitch? That is not a new question: the nationwide EPD that fell through in 2011 was supposed to already provide a solution for this. The fact that the framing of a nationwide EPD perhaps inspired the wrong associations overlooked the underlying need. Data exchange must follow the care path of the patient/client. Interoperability is not just a Dutch issue. Interoperability is an issue in virtually all Western European countries, with the exception of a few northern European states.

Over the past several years, another development has been added to this. While digitalisation had previously focused strongly on automation within an institution (which EPD or ECD to use), it has since focused on connecting different institutions (after all, we work as part of a chain). Healthcare is shifting increasingly towards value-driven care that is provided in changing networks of healthcare professionals. Because unity of language and technology is still insufficiently worked out, the exchange of data comes up against obstacles. EPD systems from different providers often fail to communicate with each other, because standards

339 https://www.nictiz.nl/standaardisatie/interoperabiliteit/.

have not been embedded in the same manner. Standards for exchange are often still inadequately implemented or accepted. And if there is a standard, such as the BasisGegevenset Zorg, which is related to the European Patient Summary, sector-specific interpretations also arise, because the standard does not tie in quite as closely as it could to the specific need. Interoperability is a permanent challenge in the diversely organised Dutch healthcare landscape.

European perspective

It has been agreed on the European level that healthcare is a national responsibility of the Member States. Nonetheless, healthcare and electronic data exchange in healthcare are important European topics. The EU has a rich history of reports and projects in the area of interoperability. In 2008, guidelines appeared for the implementation of electronic patient dossiers to securely disseminate patient data within Europe.[340] One of the key projects in this context is the European patient Smart Open Services project (epSOS), which worked on, among other things, the aforementioned patient summary and a digital prescription. The epSOS project was concluded in 2014.[341]

The interoperability in healthcare is part of the formation of a 'digital single market'. The programmes that contribute to that are ISA and ISA 2. The implementation of the European Interoperability Framework also takes place within the ISA programme. In this context — without getting lost in the forest of programmes and recommendations — it is interesting to mention the European Health Exchange Format (EHEF). The recommendation for EHEF appeared in 2019. The EHEF is primarily intended to contribute to facilitating the interoperability of electronic patient records within Europe.[342] The decade of initiatives makes it clear that with the multitude of individual national formats and standards, exchange is no easy task.

340 Recommendation on cross-border interoperability of Electronic Health Record systems (2008).

341 Cross-border health project epSOS: What has it achieved? | Shaping Europe's digital future (europa.eu).

342 Recommendation on a European Electronic Health Record exchange format | Shaping Europe's digital future (europa.eu).

Under pressure, everything becomes fluid

Over the past several months, there have been a number of publications that point to the acceleration that has occurred in eHealth and electronic data exchange.[343] The need for a different way of working has caused earlier obstacles to evaporate. Video-calling has become commonplace in a short period of time, both in first-line and specialist care. This often involved technology that has been available for years. In the Netherlands, at the request of VWS, Philips realised a Corona Portal to facilitate image exchange between hospitals, which was important at the moment that patients were being transferred. This application was only applied nationally.

From the start, apps have had a prominent place in the digital coronavirus environment. In the first weeks already after countries entered lockdown, intelligent or otherwise, energy was put into developing a coronavirus app, following suit from international examples. Singapore made its knowledge available to the world at the end of March 2020. European countries focused on an app aimed at supporting source and contact investigation. The Dutch story is well known. After the appathon in which the solutions offered were unable to satisfy privacy and security requirements, the Netherlands developed its own app, the CoronaMelder. This became available nationwide on 10 October 2020. In this context, the Netherlands is one of the countries that felt it necessary to have a statutory basis.

Within the EU, interoperability was, from the start, an important theme for supporting the international journey of the citizen. The table below provides an overview of the various European apps used to support source and contact investigation and their operability.

343 See, for instance: https://www.nivel.nl/nl/project/organisatie-van-zorg-op-afstand-coronatijd-binnen-de-huisartsenpraktijk, or: https://www.zorgvisie.nl/coronacrisis-dwingt-ook-ggz-tot-e-health-en-digitalisering/.

Countries	App	Interoperable - is this app potentially interoperable?	Interoperable - can this app already talk to another app?
Austria	Stopp Corona App	Yes	No
Belgium	Coronalert	Yes	No
Bulgaria	The deployment of a contact tracing app is not foreseen.		
Croatia	Stop COVID-19	Yes	Yes
Cyprus	A contact tracing app is under development.	Yes	No
Czechia	eRouška	Yes	No
Denmark	Smittestop	Yes	Yes
Estonia	A contact tracing app is being planned.	Yes	No
Finland	Koronavilkku	Yes	No
France	TousAntiCovid	No	No
Germany	Corona-Warn-App	Yes	Yes
Greece	Contact tracing app under development.	Yes	
Hungary	VirusRadar	No	No
Ireland	COVID Tracker	Yes	Yes
Italy	Immuni	Yes	Yes
Latvia	Apturi Covid	Yes	Yes
Lithuania	Korona Stop LT	Yes	No
Luxembourg	The deployment of a contact tracing app is not foreseen.		
Malta	COVIDAlert	Yes	No
Netherlands	CoronaMelder	Yes	Yes
Poland	ProteGO Safe	Yes	Yes
Portugal	StayAway COVID	Yes	No
Romania	The deployment of a contact tracing app is not foreseen.		
Slovakia	A contact tracing app is being developed.		
Slovenia	#OstaniZdrav	Yes	No
Spain	Radar Covid	Yes	Yes
Sweden	The deployment of a contact tracing app is not foreseen.		

Table 1: Overview of European countries and their coronavirus apps.[344]

EU Gateway

The overview shows that twenty countries have an app that is potentially interoperable. Making the app interoperable is up to the countries themselves (the Netherlands — December 2020). The European Commission published a set of guidelines in mid-May 2020 already: Guidelines on interoperability of approved contact-tracing apps.[345] These apps must satisfy the same standards (privacy, data protection, security, effectiveness, no geolocation and voluntary use). In October 2020, the EU Gateway became available, allowing information to be passed on

344 Source: Mobile contact-tracing apps in EU Member States | European Commission (europa.eu).

345 https://ec.europa.eu/health/sites/health/files/ehealth/docs/contacttracing_mobileapps_guidelines_en.pdf.

cross-nationally. The EU Gateway is intended mainly to encourage cooperation (information exchange) outside national borders. [346] People who indicate via their national coronavirus app that they have been infected also pass the code via the European server. Other national coronavirus apps retrieve these data from the server in order to be able to pass on warnings. This only applies for countries that have their own app operational. Thanks to this mechanism, as a European citizen you only need to install a national coronavirus app. Since the free movement of persons is a fundamental feature of the EU, the EU attaches a great deal of importance to this connectedness among countries. A large number of the countries are joined up to the Gateway, which it has been agreed will only exist for the duration of the pandemic. Strictly speaking, this does not involve data exchange; it is a notification function that cannot be traced back to individual persons.

World of difference

Countries worldwide are struggling with digital data exchange. The parties come up against different systems, different standards, different interpretations of a 'patient summary' and differences in language between specialist, general practitioner and nurse. The more than 300,000 medical terms from Snomed are certainly not common knowledge.[347] Across the borders, the struggle is not the sum total of countries that want to exchange data, but a multiplication of the problems these countries already have internally. What has made the difference then in the decades-long struggle and the haste that has now been made, even though countries have individually been accused of operating slowly? We point out the following circumstances:

- the COVID-19 apps were able to be built based on existing standards, whereby Apple and Google made their APIs available: the EU sought coordination in order to have their interoperability wishes tie in with the APIs as well;
- the major challenges lay not in the technology but in the privacy requirements that applied on the European and national level;

[346] In January 2021, Belgium, Cyprus, Germany, Denmark, Ireland, Italy, Croatia, Latvia, the Netherlands, Poland and Spain joined up.

347 Snomed is an international medical terminology system. Also see: https://www.nictiz.nl/standaardisatie/terminologiecentrum/snomed-ct/.

- the wish of the member states to facilitate the free movement of persons again as quickly as possible;
- the solidarity felt nationally and internationally to shorten the first wave and prevent a second wave.

Conclusion

Every text is tied to the time in which it was written: the irony of the 20 countries that joined up to the EU Gateway is that the interoperability of these COVID-19 apps is mainly of value if there is international travel. The change of colour code from yellow to uniform orange naturally discourages the free movement of persons across borders. Just as during lockdown there are fewer notifications from the CoronaMelder app, that has the same effect internationally. It may be that the speed of vaccination reduces the effectiveness of the various apps, but the lesson for future interoperability issues lies in breaking free from the technological but rather political-social rigidity that has existed on this topic for years.

The expectation that COVID 19 is not an isolated case but rather a harbinger of more frequently occurring infectious diseases means that we should be focusing more precisely on national and international data exchange. If IC patients are transferred from the Netherlands to Germany, then EPD systems should preferably also be internationally interoperable. Although it must naturally be considered in this context whether the numbers would justify the investment.

Some considerations

Interoperability in healthcare remains a challenging topic in which existing standards, ageing information systems and infrastructures, both nationally and internationally, pose obstacles. In perspective, there are in any event three takeaways:

- **Standards.** National and international interoperability thrives with the use of standards. Precisely because healthcare is reserved for the Member States, making agreements on this poses a challenge. IHE and HL7 are trying to take steps in that regard to achieve more connection internationally.[348] The coronavirus crisis has once again made the need for international standardisation explicitly clear.

348 See https://www.ihe.net/ and https://www.hl7.org/.

- **Aiming for new technology.** Interoperability is already coming up against the limits of existing systems and infrastructures nationally. The COVID-19 apps make it clear that with a new development in which building can take place outside of the existing systems, convenient forms of exchange are possible. Think also of open source and API in this regard.

- **Think of secondary use.** An area in which faster steps may need to be taken, from the perspective of reuse and effective prevention, is in the area of open data. On the one hand, there is the interoperability that can be expected in order to improve the direct care for patients. On the other, there is a strong need to use open data in the context of research or improving treatment methods. Here, too, COVID-19 has been a good push for the development of portals (nationally and internationally).[349] The foundation is there, now it is a matter of moving forward.

349 https://data.europa.eu/euodp/en/apps and https://www.ecdc.europa.eu/en/covid-19/data-collection.

18 Confidence in sharing personal data

Erik Beulen

The Dutch Data Protection Authority (Dutch DPA) initially advised against the use of the COVID-19 notification app. Despite the privacy by design incorporated in the design, there were three serious objections. Firstly, the technical processing is based on the Global Apple Exposure Notification framework, whereby it cannot be sufficiently determined whether Google and/or Apple process personal data. Secondly, the Dutch DPA advised that a specific and clear statutory basis be created for the processing. Finally, the back-end server also needed to comply with the GDPR standards. In the United Kingdom, for example, there were similar concerns, but the regulator there was more positive. The dangers of digital monitoring and tracking are recognised worldwide, however. Modifications have since been made to the COVID-19 app to address the Dutch DPA's objections. On 4 February 2021, over 4.5 million people in the Netherlands had downloaded the app. A large number of residents apparently has confidence in these mobile applications. That raises more generally the question of how willing consumers are to share personal data with organisations, including commercial ones. How do data ethics contribute to consumer confidence?[350]

Explanation

Reliable artificial intelligence satisfies the following three criteria: lawful, ethical and robust,[351] whereby robustness encompasses both technical aspects and the social environment. In relation to data mining, a large number of stakeholders are involved in the privacy debate, and not just the organisations that use this information technology and the government organisations that provide (legal)

[350] This chapter was written on the basis of the keynote lecture that the author presented to the Data Driven Marketing Association — 'Digital Talk: data ethics and consumer confidence' — on 26 January 2021.

[351] https://ec. europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai

frameworks, but also individual managers and employees of the companies involved, customers and end users, competitors and society as a whole.[352] The advantages of sharing data and artificial intelligence are clear:

1. improved service provision by the addition of data elements to products and services;
2. more efficient and more effective production of products and services.

And yet citizens have doubts about sharing their personal data with commercial and other organisations[353]. Naturally, the willingness to share varies from sector to sector: hospitals and governments score high, while social media — Facebook, for instance — score significantly lower. What is striking in this is that in a survey by Deloitte,[353] retail received a higher score than the financial sector. This could be explained by the fact that customers who share their personal data are offered advantages. Loyalty cards are, after all, commonplace at retailers.

In order to boost this willingness to share personal data, organisations must also strengthen their data ethics. It is important in this context that organisations know where they stand at the moment and how they can improve this in a systematic manner, whereby frameworks, such as the British Data Ethics Framework,[354] can provide support. This framework is based on three principles: transparency, accountability and fairness.

Market and technical developments

There are three market developments that must be taken into account when improving data ethics. Low data quality, an increase in the number of data-driven decisions and growth in 'data democratisation'[355] pose a threat to improving data

[352] Dean, Matthew D., Dinah M. Payne, and Brett J. L. Landry. 2016. 'Data Mining: An Ethical Baseline for Online Privacy Policies.' Journal of Enterprise Information Management 29(4):482-504.

[353] https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Consumer-Business/gx-consumer-data-give-and-take.pdf

[354] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/923108/Data_Ethics_Framework_2020.pdf

[355] Data democratisation is a development whereby data are made available to managers and employees. With these data, they can make their own analyses and take decisions on the basis of these data.

ethics and, as such, have a negative impact on the willingness to share data.[356] Organisations can work on improving data quality by focusing primarily on improving data management and the automation of analytics. In addition, the involvement of operational management ensures improvement in data-driven decisions. That is sorely needed, because the percentage of data-driven decisions by organisations will increase significantly over the coming years.

In order to ensure that data democratisation takes place smoothly, it is essential to invest data ownership properly in an organisation. Appointing a Chief Data Officer (CDO) helps provide direction and set up policy. In the long term, this role will be incorporated and transformed from a C-level role to a supporting role on management level.

In addition to the market developments, the technological developments are also taking place rapidly. The rise of machine learning and deep learning means that the outcomes of artificial intelligence are less predictable and traceable. Naturally, this lowers consumer confidence and the willingness to share personal data. The key difference between machine learning and deep learning is that in deep learning, information independently tries to interpret and organise (new) data. With machine learning, data are interpreted and organised in accordance with the programmed algorithms.

Platform economy

With companies like Amazon, Uber and AirBNB as frontrunners of the platform economy, this business model has grown into one of the most important ones of the moment. The distinction is made here between the platform, producers and consumers, whereby organisations sometimes opt for a combination of platform and the role of producer. Access is often also granted to other independent producers.[357] A fee is charged to the producers and/or the consumers in exchange for making the platform available. It is important that the platform ensures a sufficient number of producers with an attractive offering and a sufficient number of consumers who are interested in purchasing the products and services from the producers. This makes content curation by the platform essential. In this context, the platform moderates and ensures that the quality of the products and services offered by the producers is appealing for the consumers. The platform also binds

[356] https://itexecutive.nl/hpdo/excelling-in-the-data-economy-demonstrate-data-driven-leadership/

[357] Van, A. M. W., Parker, G. G., & Paul, C. S. (2016). Pipelines, platforms, and the new rules of strategy. Harvard Business Review, 2016 (April).

appealing customers to the platform, in turn ensuring that it is an attractive proposition for producers to offer their products and services via the platform.

A platform's strategy to bind both producers and consumers to the platform is important. During the launch of a platform, incentives are often offered to both producers and consumers. The accessibility to the platform and ease of use is also important, whereby it should be noted that information security is also crucial. Security measures, such as authentication, often have a negative impact but are indeed essential for customer confidence.

Regulation and lawsuits

Recently, the criticism of platforms has grown, and there have been a number of lawsuits. An example is the European Commission scrutinising Amazon.[358] The US-based company is accused of abusing its dominant market position.[359] Amazon uses non-public data from independent sellers (producers). In the indictment, the European Commission alleges that these data are widely and automatically collected and made available to Amazon employees. Employees reportedly also use the data to improve the products offered by the company and the conditions relative to the independent sellers. Amazon is also accused of favouring independent sellers who make use of the packaging, shipping and handling services[360] offered by Amazon. It should be clear that such lawsuits have a negative impact on consumer confidence and consumer willingness to share personal data with organisations.

This is also recognised by the European Commission. At the end of last year, the Digital Service Act & Digital Market Act was announced.[361] The objective of the Digital Service Act is to protect consumers and their fundamental rights online, to ensure transparency and a clear accountability framework for online platforms, and to promote innovation, growth and competitiveness within the unified market. This legislation is primarily aimed at platforms that reach more than 10% of the residents of the European Community. The Digital Market Act is aimed at creating a transparent online market and mainly contains obligations for platforms. This legislation will contribute positively, but aside from this legislation, it is important that organisations themselves start taking steps.

---

[358] https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2077

[359] Article 102 of the Treaty on the Functioning of the European Union (TFEU)

[360] FBA sellers

[361] https://ec.europa.eu/digital-single-market/en/digital-services-act-package

Finally

We still have a long way to go at the moment. Consumers must have confidence in an organisation before they share their personal data. Surveys show that only half of the participants have confidence in artificial intelligence interactions and that over 40% will opt for human interaction after a bad experience with artificial intelligence interactions.[362] This makes clear how thin consumer confidence is in organisations in order to share their personal data.

The European Union gives organisations seven focal areas for using artificial intelligence in a beneficial manner.[363] Elements from the data ethics framework reappear here as well. There is also explicit attention for human/management supervision, social and environmental well-being, robust technical solutions (built and maintained under architecture) and privacy and data governance. The governance consists of an unambiguous policy and clear guidelines, the installation of an ethical algorithm committee and a process whereby the algorithms are periodically scrutinised.[364] It is only with attention to these points that consumer confidence in artificial intelligence algorithms and willingness to share personal data will be increased in the future.

Some considerations

- More than 4.5 million Dutch people have now downloaded the COVID-19 notification app. You could argue that citizens' willingness to share their personal data can be explained by citizens' belief that their own and our collective health would benefit from the use of the app. But it would be good to do further research into their actual motivations.

- The initiatives of (European) governments to protect consumers will only have a positive effect on consumer confidence and a willingness to share personal data in the medium to long-term. This legislation has far-reaching consequences for many organisations. These will need time to adapt their service provision; even judicial enforcement takes time. As such, it seems likely

[362] https://www.capgemini.com/wp-content/uploads/2020/10/AI-and-the-Ethical-Conundrum-Report.pdf

[363] https://ec. europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai

[364] https://hpdo.nl/research/2020/12/04/paper-demonstrating-data-driven-leadership/

that this new legislation will only have a positive effect in the medium to long term.

- To ensure increased consumer confidence, organisations can also make their own progress, in addition to the adjustments made as part of the enhanced legal requirements. In particular, improving data quality should be the highest priority. Many organisations, however, are lacking a vision and strategy to work on these improvements in a structured manner. Giving a mandate to a Chief Data Officer is a good first step. This officer can, as quartermaster, lay the foundation for implementing improvements that, in time, will increase consumer confidence and willingness to share data. To be continued!

19 Medical apps and patient rights

Bert Morsink

An important development in the ever-progressing digitalisation is the rise of mobile devices such as smartphones and wearables and the applications or apps on these devices. Apps are now part of our daily life and are used for various applications, such as monitoring and improving our health. Health apps are generally freely available, are offered to consumers without the involvement of healthcare providers and have a supportive and obligation-free character. There are also apps, however, called medical apps in this chapter, that are used in the context of medical treatment. It could be argued that the apps that are used in public healthcare to combat the coronavirus, the so-called coronavirus apps, could also be seen as medical apps. It could also be argued that contact-tracing apps, such as the CoronaMelder, should only be seen as tracing apps. The technological developments are taking place rapidly at the moment. Apps are being given increasingly more functionality and (artificial) intelligence. The use of medical apps can have advantages for patients and healthcare providers and can bring the healthcare system as a whole to a higher level of quality and efficiency. The use is not without risks to the patient, however.[365]

Patient rights

Medical procedures[366] and the use of devices[367] therein are strongly regulated by legislation and regulations. An important basis for this legislation and regulation

[365] This chapter is based on L.H.A. *Morsink, Patiëntenrechten bij het gebruik van medische apps [Patient rights in the use of medical apps]*, Weert: Celcus Juridische Uitgeverij, 2020.

[366] A medical procedure is defined in this chapter as a procedure regulated by the Medical Treatment Contracts Act (WGBO), Healthcare Quality, Complaints and Disputes Act (Wkggz) and Individual Health Care Professions Act (BIG Act).

[367] Some procedures in the context of public healthcare can also be considered medical procedures. The Medical Device Regulation (MDR) also classifies devices for the purposes of preventing and diagnosing disease as medical devices. Finally, the guidelines of the RIVM are programmed into the coronavirus

are the fundamental rights laid down in human rights treaties and the Constitution. Legislation and regulations are supposed to protect these fundamental rights, but the question is whether they currently do so sufficiently in this rapidly developing area.

A medical procedure can be subject to a treatment contract regulated by the Medical Treatment Contracts Act (WGBO). The parties to a contract envision arriving at a satisfactory result in cooperation with each other. The quality of the care provided by a healthcare provider to a client is provided for in the Healthcare Quality, Complaints and Disputes Act (Wkkgz). The Individual Healthcare Professions Act (BIG Act) also focuses on the quality of healthcare, among other ways by protecting patients against inexpert and careless treatment by healthcare providers. Soon a new European regulation for the development and use of medical devices will come into force, the Medical Device Regulation or MDR. The more stringent rules were to take effect from 26 May 2020, but their introduction was postponed by a year.[368]

Shared decision making

A recent amendment to the Medical Treatment Contracts Act (WGBO) stipulates that the care provider must discuss the effects, risks, schedule and alternatives in relation to the treatment with the patient in a timely manner, must become thoroughly acquainted with the personal situation and needs of the patient and must invite the patient to ask questions. This is based on the concept of shared decision making and requires continuous interaction between care provider and patient. In this context, the care provider is required to gear discussions to the individual patient's subjective experience, capacity to understand (including reading and writing skills), cultural background and needs and situation.

apps. On the basis of this, these apps can be seen as medical apps. See also Mr. dr. M.C. Ploem & mr. dr. T.F.M. Hooghiemstra, Corona te lijf met een app [Tackling coronavirus with an app], Tijdschrift voor Gezondheidsrecht [Journal for Health Law] 2020(5),), p. 509-523.

[368] This was done to give more latitude to the measures to combat COVID-19. See the explanation from the Inspectorate for Health and Youth Care (IGJ) at https://www.igj.nl/actueel/nieuws/2020/05/07/nieuwe-wetgeving-medische-hulpmiddelen-jaar-uitgesteld.

Human dignity and equality

Human dignity is interpreted in roughly two ways within health law: dignity as the norm when it comes to personal autonomy and dignity as the norm when restricting human actions in order to prevent exceeding the limits of (absolute) human dignity.[369] Within health law, the principle of equality is primarily related to preventing disadvantage in access to health care and the distribution of scarce resources.[370] Equal access to care also means that accessibility is not determined by personal characteristics such as knowledge, skills, background and means. People with a need for care are often vulnerable and dependent on others to obtain care and support. In the care relationship as well, there must be as much equality as possible.

(Relational) autonomy

The right of self-determination is seen as perhaps the most important right of the patient. This is reflected in the right to information and the right to give consent (together: informed consent). In health law, self-determination is of particular importance, because the patient is often dependent on the care provider and the healthcare system, medical treatments can sometimes be deeply invasive and institutions and government can exercise power over the individual. The patient must have the freedom to make his or her own choices. Freedom of choice does depend on decisional competence or incompetence, individual financial capacity, illness risks and disease burden, the self-determination right of others, the available possibilities, the professional standard of care providers and societal beliefs.[371] Medical and technological progress can expand freedom of choice but also limit it. Increasing predictability in relation to health can, for instance, increase social pressure to display certain behaviour.

In order to know what (real) need he or she has, help from others is often indispensable for the patient. Care providers must therefore not only engage in

[369] A.C. Hendriks et al., *Het recht op autonomie in samenhang met goede zorg bezien [The right to autonomy considered in combination with good care]*, in: Tijdschrift voor Gezondheidsrecht [Journal for Health Law], 2008, p. 2-18.

[370] H.J.J. Leenen et al. (ed.), Handboek Gezondheidsrecht [Health Law Handbook], The Hague: Boom juridisch, 2017.

[371] H.D.C. Roscam Abbing, 'De persoonlijke vrijheid en waardigheid van de patiënt' [The personal freedom and dignity of the patient], in Grondrechten in de gezondheidszorg [Fundamental rights in healthcare], Houten: Bohn Stafleu van Loghum, 2010, p. 25-34.

providing information, but also act as counsellors for the patient and help think of options/solutions. Good care provision implies that shared decision making is paramount. In this process, the patient is constantly developing, among other things under the influence of the choices made, and must be regularly asked whether a choice is still appropriate.[372]

Advantages

Medical apps make it possible to provide help and support very directly, in everyday situations. The use of medical apps (and e-health in general) can also contribute to improving the efficiency of healthcare. In order to guarantee the affordability of healthcare, there is a constant need for cost reduction. This can also put accessibility under pressure.

Supported by the functionality and intelligence of medical apps, the patient is put more in control. The patient is at the helm, and the medical app, operated by the patient, takes over part of the care provision and information provision to the patient. For this part, the patient is in essence his or her own care provider. By shifting a bit of the care and care management to the patient via the medical app, costs can be limited without the patient experiencing any disadvantage from this, provided the quality is sufficient of course. And that is the sore point at the moment, of course.

Risks

Despite the risks, there is little research being conducted into the use of medical apps. A few risks ascertained in studies are explained briefly below. [373]

The current quality of medical apps is often insufficient or unclear. This lack of clarity is also related to the fact that more and different parties such as app developers, platform providers and data scientists are becoming involved in the care provision. Assessing quality is also difficult if an app uses artificial intelligence, because the functionality is not constant in that case.

The growing technological capabilities means people are being observed, analysed and influenced in all sorts of ways. Artificial intelligence enables apps to

[372] A.C. Hendriks et al., *Het recht op autonomie in samenhang met goede zorg bezien [The right to autonomy considered in combination with good care]*, in: Tijdschrift voor Gezondheidsrecht [Journal for Health Law], 2008, p. 2-18.

[373] Centre for Ethics and Health, Health apps and wearables The ethics of e-health part I, The Hague: Centre for Ethics and Health, 2020.

respond to human behaviour. This can blur the lines between voluntary and coercive. There is little yet known about how medical app use influences patient behaviour.

Especially people with low health skills run the risk of losing an overview of their own health because of (an abundance of) signals from the apps. This can prompt people to make use of healthcare possibly too often or in fact too little.

The optimal level of self-management for a patient depends on a person's capabilities and on societal attitudes. Apps can give the impression that health can be fully managed by individual actions. Advice and conclusions from apps also have a moralising effect.

It is far from the case that all medical apps are accessible for everyone. Apps for seriously ill patients and people with low health skills are scarce. In addition, most apps focus on a single condition, and the burden can become too great for people with multiple conditions. Apps that are mainly suitable for people with high health skills can ultimately increase the social (health) differences. If people have no sympathy for those who are not willing or able to use these apps, solidarity also comes under pressure.

CoronaMelder

The analysis of the CoronaMelder app from the perspective of patient rights yields two important points for attention. First of all, quality, on which there is much discussion. The reliability of the app, as mentioned on the informational website, is not impressive, and the practical tests conducted yielded hardly any usable results. The CoronaMelder app is a device with the aim of preventing illness and is probably a medical device in accordance with the MDR regulation. In that case, the app will soon have to satisfy stringent quality requirements.

Another important point for attention is the voluntariness of use. There is no legal framework for mandatory use and therefore restriction of freedom.[374] There is also the danger that not using the app could have consequences, for instance by denying access to certain spaces. Requiring the use of the CoronaMelder app has indeed been legally excluded in the Temporary Act on the COVID-19 Notification Application. People can also adjust their behaviour to the possible consequences without these actually taking effect, for example in the form of the chilling effect. In this specific case, that is indeed more or less in line with the

[374] According to Article 8(2) ECHR.

coronavirus measures in relation to social distancing, but to what extent is this behaviour voluntary?

The effectiveness of the app, which has still not been demonstrated, is a condition for justifying the breach of personal privacy.[375] This effectiveness will therefore have to be continuously monitored.

Assessment of medical apps in general

The investigation into medical apps yields a worrying picture. Roles and responsibilities are not always clear, and information on choices is insufficient. There is a danger of fragmentation, because more parties are becoming involved in the care for a patient, medical apps are focused on specific procedures and the apps do not 'work together'. The effect and information provision is often not attuned to the patient's personal characteristics and situation, with potential inequality and inaccessibility as a result. Formal and actual decision-making possibilities are not monitored, the granting of consent is unclear and there is hardly any interaction.

There is no shared decision making, and the patient being in control seems for the time being still a dream. Nor is there any monitoring of incorrect use or abuse, let alone active intervention if that is required, for example if human dignity is in jeopardy. Identity and informational privacy are also insufficiently protected, and in public healthcare, there may be restriction of freedom without a statutory basis. Finally, the supervision on all of this falls short.

Conclusion

The danger of today's more or less uncontrolled developments is that the 'patient' will in future still mainly consist of data and controllable behaviour, whereby control takes place on the basis of indicators that fall outside the patient and his/her sphere of influence. This patient is assumed to be in control, but in fact artificial intelligence takes over the helm. In short, patient rights are in danger!

[375] Mr. dr. M.C. Ploem & mr. dr. T.F.M. Hooghiemstra, Corona te lijf met een app [Tackling coronavirus with an app], Tijdschrift voor Gezondheidsrecht [Journal for Health Law] 2020(5),), p. 509-523.

Recommendations

- The protection of patient rights can be improved through professional standards and legislation and regulations. What remains are aspects that are more difficult to 'pin down'.

- It concerns mainly possibilities of control for the patient who is supported by all sorts of medical apps and the (possibly undesired) influence of medical apps on human behaviour, partly as a result of the use of artificial intelligence. This also touches more on the development of the healthcare system as a whole, and this implies an important role for the government.

- The government can steer this development by, among other things, setting up guidelines, encouraging and performing research, developing and evaluating policy and policy theories, and carrying out legislative evaluations.

20 Some viewpoints on RadarCOVID in Spain

Carlos Juiz

The RadarCOVID contract tracing application of the Spanish central government was launched in order to communicate to close contacts of someone who has been diagnosed with COVID-19. In case of infection, it is a safe way to notify others without having to reveal identities. Such an app did not seem as interesting as the government had hoped for citizens since downloads are limited in comparison to smartphone popularity in Spain. However, the start of the current national vaccination process could very well be a second opportunity to attract citizens to download and use the mobile application with additional functionalities.

Working of the app

The RadarCOVID contract tracing app can be downloaded through the official Apple and Android stores and communicates via Bluetooth technology. Every 5 minutes, the app sends a random code to the nearest mobiles. These codes do not contain any personal, geolocation or GPS information. The app also receives the codes of the nearest mobiles that have the app installed. If two or more mobiles have been close for more than 5 minutes, codes will be exchanged. The app remembers the codes sent and received during the last 14 days. As of the fourteenth day these codes will be removed. These codes are only stored on the mobile itself and are not sent to any external server.

The citizen who has been diagnosed is asked if he or she has the app installed. If the citizen wishes and has the app installed, they will be provided with a disposable code so that they can voluntarily decide if they want to share with the rest of the users that he or she diagnosed positive for COVID-19. If the citizen decides to share this information, he/she will only send the random codes generated by himself / herself. No personal information will ever be shared. Each app will update the list of positive codes for recent COVID-19, and will verify that there is no record of positive codes on your mobile. If there is a contact in each app's own record, the application will analyze the distance and duration of the

contact. If a user meets the risk contact criteria (more than 15 minutes within 2 meters over 24 hours), it will notify the user so that they can contact the health services to receive the appropriate instructions.[376]

Technology details

The Spanish government developed RadarCOVID,[377] as a free app available for Android 6+ and iOS 13.5+. The use of the app is on a voluntary basis. It is based on an anonymous contact diary that logs the various encounters via wireless Bluetooth Low Energy (BLE). The system architecture is based on the decentralized Google/Apple API. The source code of the app can be found on GitHub, and is open source with the Mozilla Public License, Version 2.0.[378]

No registration or other personal information is needed to install and use the app. During the app installation, a random Universally Unique Identifier (UUID) is generated by the app. The app updates this identification every 10 to 20 minutes. The details regarding the privacy policy of the app can be found at the webpage[379] of app owners, i.e. the General Secretariat for Digital Administration (SGAD), which is dependent of the State Secretariat for Digitalisation and Artificial Intelligence of the Ministry of Economic Affairs and Digital Transformation. The servers are located in the European Union.

RadarCOVID tracing app effectiveness

One recent study,[380] published in Nature Communications, assessed the effectiveness RadarCOVID, following a 4-week experiment conducted in the Canary Islands, Spain between June-July 2020. For the experiment, funded by the Secretary of State of Digitalisation and Artificial Intelligence (SEDIA), the researchers simulated a series of COVID-19 infections in the capital of La Gomera, San Sebastián de la Gomera, to understand whether the RadarCOVID app technology could work in a real-world environment to contain a COVID-19 outbreak.

They found that over 30 per cent of the population adopted the technology and it was able to detect around 6.3 close-contacts per infected individual, which was over two times higher than the national average detected using manual contact

[376] https://radarcovid.gob.es/home

[377] https://www.hindawi.com/journals/wcmc/2020/8851429/

[378] https://www.mozilla.org/en-US/MPL/2.0/

[379] https://radarcovid.gob.es/politica-de-privacidad

[380] https://www.nature.com/articles/s41467-020-20817-6

tracing alone. However, the researchers suggest that the app's success is dependent on effective national and local communications campaigns to encourage people to download and use the app in the first place.

Fewer downloads than expected

More than 85% of the Spanish population owns a smartphone, of which 17% have downloaded the contact tracing application. According to some official estimates, if 20% of the population downloaded the application, the impact of the pandemic could be reduced by 30%. However, this level of download has not occurred in Spain according to various studies. Despite this, Spain was the fourth country in downloads in September 2020 and the most downloaded app in the Play Store for many days.[381]

The first data on registered unique visitors were those relating to the month of August 2020. During that period, the application obtained 3.5 million unique visitors, figures that have been increased by 10% in its second month of life. In September 2020, the app registered 3.9 million unique visitors. Extrapolating these results to the total number of Internet users in our country, we would be talking about 1 in 10 people in Spain having used the application since its launch.

Currently RadarCOVID is available in all autonomous communities. However, unique visitors from all over Spain show their interest in the application. In addition to this, the demographic data recorded during these two months also shows us more details about the audience of RadarCOVID. Thanks to the affinity index, we observe that the audience of the application is mainly female and that it decreases proportionally with the age of the user.

It should be mentioned that this data is relative to the use of the application, not the total number of downloads. Currently, the application is available in the two large virtual stores of applications for mobile devices: Google Play and Apple Store. However, it is one thing to download an application and another to use it.

Individual responsibility

When a citizen tests positive, it is up to them to report the test result. It is thus a voluntary decision and at that point it no longer brings them any individual benefit, since individuals do not perceive that social benefit from the use of the app. The effectiveness of the app is evident where its use has been imposed on a mandatory

[381] https://www.europapress.es/portaltic/software/noticia-solo-99-poblacion-espana-smartphones-descargado-aplicacion-radar-covid-20201009113731.html

basis, as in China, but it is difficult to evaluate its effectiveness where its use is voluntary. Not even in countries with a technological and epidemiological history, such as Singapore, are they reaching a high level of usage (it has not exceeded 16 or 17% of the population) as it is a mere recommendation. The irrelevant perception about the app among users may derive from information about possible administrative mismanagement or be related to privacy, even though the app is secure.

Figure 1. Radar COVID appearance[382]

Code released

On 9 September 2020, the central Government made the source code of RadarCovid public – as open-source software[383] – after computer experts requested it as an exercise in transparency, to learn about the mechanism of the application and to check if privacy of its users is guaranteed. Analysis of this programming code revealed traces of Firebase in the application, a Google tool for creating applications that sends error reports with information about the phone model, time and use mode. In this regard, SEDIA sources clarified Firebase was only "used during

[382] https://marketing4ecommerce.net/analisis-app-radar-covid-errores-diseno/

[383] https://github.com/radarcovid/

the 'testing' phase to accelerate the development of the app by detecting possible errors, nothing more. (..) In fact, in the current version of the application it is no longer there. Its use was limited to that and no user data has ever been collected or used in any way", they point out.[384]

Why RadarCOVID may not be downloaded as much as expected

If we try to analyze the consolidated reason that the download and use of the official Spanish COVID-19 contact tracing app do not meet the expectations of the health authorities, the following factors play a role:

- late deployment in comparison with other EU countries
- limited compatibility with older OS versions
- some privacy breaches at the start, although fixed rapidly
- a single point of process failure, because without the diagnosis code, sent by the healthcare information systems, the app has no sense
- app design does not seem to be user-oriented
- accessibility-related problems at the start of the deployment, but these are also fixed
- not being very popular because public address communication campaigns failed to reach citizens

Conclusion

The relatively small number of downloads and usage,[385] the lack of implementation throughout the country at the same time and the institutional campaigns not pushing the individual responsibility are three key reasons for RadarCOVID for being just another app on Spanish mobiles and not becoming an effective tool in the fight against the coronavirus. The main reason for rejecting the application, however, is related to its real usefulness. Additional concerns are based on fears about privacy violations, although this suspicion is not based on any reality.

Since it is a mobile app, the strategy for consolidating the number of real users must be accompanied by the incentivisation of the central government to not only download it but also to make use of it in the context of citizen's responsibility. On the other hand, diagnose codes must be known and verified in some extent

[384] https://www.abc.es/tecnologia/moviles/aplicaciones/abci-tres-motivos-radar-covid-todavia-no-eficaz-202010021655_noticia.html?ref=https:%2F%2Fwww.google.com%2F

[385] https://radarcovid.gob.es/estadisticas/descargas-radar

without compromising privacy. In the current scenario, with the first vaccinations deployed in Spain in January 2021, many experts believe that RadarCOVID could have another complementary approach, by also offering information on how to get vaccinated or to carry on some information about it.

21 Competition aspects of app stores

Rob Ludding

Competition law is having difficulty getting a grip on the digital economy. Algorithm-driven pricing makes consultation on prices and conditions between competitors in 'smoke-filled rooms' superfluous, and the takeover of promising start-ups often stays under the radar of merger control because of the target's modest turnover (at the time). In practice, this means that of the three instruments that the competition authority has at its service, the only one that remains is the ban on abusing a dominant position. The ban on anticompetitive agreements and mutual coordination, as well as supervision on certain mergers and takeovers, emerge not to work or not to work sufficiently in this context. That is why the call for additional correction instruments is growing ever louder. We analyse the dominant position of the Apple App Store and Google Play Store and formulate the competition objections to these. This takes place against the background of the rollout of the CoronaMelder app. The Dutch government was forced to use the app stores of Apple and Google for this. [386]

Network effects

The GAFAM companies — Google, Apple, Facebook, Amazon and Microsoft — are all multifaceted platforms on which supply and demand meet and so-called network effects arise. Network effects drive market power. The network effect can be illustrated with reference to the example of a bank (the platform) that issues a credit card. On this issue, two groups of takers can be distinguished: the customer who wants to acquire the card and the shop that must accept the card. The more customers who present the card, the more shops will (have to) start accepting the card, after a certain amount of time. And because more shops accept the card, more customers will want to acquire it. This process reinforces itself, with the result that after a short period of time has elapsed, the card can occupy a strong market

[386] With thanks to Sonja Geldermans for her critical support.

position, aside from its objective qualities compared to competing payment products. No one wants to be without it.

This is also how it works for the app store: the more app providers in the app store, the greater the appeal of the store, the more customers in the store and the more apps are downloaded. This deliberate driving of network effects by internet platforms is referred to with the slogan 'get the bandwagon rolling'. If a platform has thus attained a virtually unassailable market position, the optimal exploitation of that position can begin. And with the current state of regulation, it is not until this point that regulators and courts can intervene.[387] The damage has already been done at that point.

Complaints and investigations

In March 2019, Spotify filed a complaint against Apple with the European Commission on account of abuse of the dominant position of Apple's App Store.[388] That abuse reportedly consists of favouring Apple's own music streaming services Apple Music and iTunes over Spotify's service, mainly fee-wise. The complaint was supported by (among others) providers of video streaming services such as Netflix and traditional news media, who complained about Apple News, in essence with the same accusations. The European Commission is investigating the case.[389] Also in 2019, the Netherlands Authority for Consumers & Markets (ACM) published its lengthy 'Market study into mobile app stores'.[390]

The ACM study, coming from a competition authority, is broader than what could be expected of the European Commission: not only competition issues but also matters such as consumer protection and the proper functioning of telecom

[387] Decision of the Commission of 18 July 2018 (Case AT.40099 — Google Android); decision of the Commission of 27 June 2017 (Case AT.39740 — Google Search (Shopping)); decision of the Commission of 20 March 2019 (Case AT. 40411 — Google AdSense for Search).

- Bundesgerichtshof (Germany) 23 June 2020, Facebook, KVR 69/19

- https://www.declercq.com/kennisblog/duitse-facebook-zaak/

[388] D. Ek, 'Consumers and Innovators Win on a Level Playing Field', *newsroom.spotify.com* 13 March 2019. See also F. Bostoen and D. Mândrescu, 'Assessing abuse of dominance in the platform economy: a case study of app stores', European Competition Journal 2020, vol. 16, nos. 2-3, 431-491.

[389] European Commission, Antitrust: Commission opens investigations into Apple's App Store rules, press release 16 June 2020.

[390] In English, to facilitate communication with foreign regulators, the European Commission and the companies involved ACM, *Marktstudie appstores*, ACM/18/032693 (11 April 2019).

markets (European Regulation 2015/2120 on open access to the internet) are discussed.

The study determines that these days, the smartphone is in fact an indispensable instrument for consumers to access services and content on the internet. This conclusion is supportive for the entire report, but there is something to be said in terms of this: consumers can also use a browser to access the internet and log in directly to the website of their (ultimate) choice. But one does have to go to some effort to do that. The choice for an app appears to perhaps be more a question of convenience than necessity, therefore.

Dictating terms

That does not apply for all apps, of course, and in particular not for the CoronaMelder, the Dutch contact-tracing app that exists precisely by the grace of the mobility of its users. The ACM's report is weakly reasoned on this crucial point of indispensability, however. On top of that, the ACM determines that Apple in particular is doing everything technically possible to prevent games and video content from appearing directly on the user's smartphone via the browser and being captured there as an app (refusing Adobe Flash). The ACM does not attach any clear consequences to this observation. Whatever the case, according to the ACM, access takes place virtually exclusively via online platforms, the apps.

With their smartphone operating systems — iOS and Android — and the linked App Store and Play Store, Apple and Google have acquired an extraordinarily strong position: an app provider who wants to reach the Dutch public on mobile phones must have a presence in both app stores. The same goes for the CoronaMelder app. Apple and Google can dictate the terms. For instance, we see further-reaching limitations of liability, the right to imitate customers' apps and the obligation to use an in-app payment system, which keeps essential customer information from the app provider. The installation of app stores developed by third parties is either not possible (Apple) or is complicated (Google). For all of this, see, more specifically, the aforementioned decision of the European Commission in the Google Android case. And here we see network effects: the more apps in the app store, the more visitors for the platform and the more appealing this platform becomes for the app providers (and for Apple and Google).

Closed marketing systems

In different ways, Apple and Google keep a strong grip on the closed nature and by extension the quality of their ecosystems. It is no surprise that both invoke the

need for quality control to dismiss complaints from app providers about unreasonable access terms and conditions. It is important to realise in this context that Google and Apple have very different business models. To put it simply, Apple is primarily a hardware producer, with a growing share in service provision. Google is in essence a collector of data, which it commercialises for advertising purposes. Nonetheless, both have a similar interest in keeping a grip on access to the app store: admitting as many visitors as possible who bring with them money (Apple) or data (Google).

It should be emphasised in this respect that offering apps via site loading bypassing the app store is either impossible (Apple) or practically problematic (Google).

Serious objections

There are serious objections to how both app stores currently function.[391] There is, first of all, the approval process for admitting newly developed apps to the app store, which is not very transparent. Clear criteria for admission are often lacking and direct communication with specialists from Google and Apple is often not possible, so that the developer is left in the dark as to the exact reason for rejection. There are also often problems with the interoperability with the operating system or certain phone functionalities, which are difficult to solve without proper communication. According to app developers, the ranking of the apps in the app store is also often opaque, consequently the proprietary apps of Google and Apple are favoured.

Another important point of concern are the commissions that app providers have to pay Apple and Google on sales via their apps: 30% for services rendered via the phone. It is remarkable — but the ACM seems not to make any point of this — that both charge the same percentage. As mentioned, both also disallow payment methods outside the app.

But what is perhaps the biggest objection from a competition perspective is the direct competition that Google, but in particular Apple, poses with its own apps in relation to similar third-party apps in its app store. The fact that the proprietary apps do not owe any similar commission — even aside from other advantages they enjoy — points to impermissible distortion of competition. It is as if the market master itself is operating a few stalls as well. This is the essence of Spotify's

[391] European Commission, 'Europe fit for the Digital Age: Commission proposes new rules for digital platforms', press release of 15 December 2020.

complaint, and the ACM shares this concern as evidenced by its press release from 11 April 2019: it is going to investigate Apple's market actions in relation to its app store.[392] We will still be experiencing some interesting times around the app store.

Conclusion

At this moment, our government is entirely dependent on the cooperation of Apple and Google for the rollout and functioning of the CoronaMelder app, a technical instrument deemed necessary to protect public health, for which the government bears responsibility. That applies for the special application programming interface (API) that the two parties developed jointly, but also for inclusion of the app in the App Store and Play Store, respectively. The current dominance of these digital platforms, in their current form, is questionable under competition law. This means that the refusal to admit an app or the imposition of admission terms that are not objectively necessary can be prohibited abuse of a dominant position, which is unlawful towards the government.

In conclusion

- The current investigations by the European Commission (Spotify/Apple) and the ACM (Apple) are expected to result in important improvements on at least three points.

- The conditions for admitting apps developed by third parties to the stores will have to be objective and transparent.

- Stores developed by third parties will also be admitted under fair and verifiable legal conditions.

- Finally, rules will apply that prevent proprietary apps of Apple and Google (and businesses affiliated with them) from competing unfairly with third-party apps in their store. Favouring proprietary apps will no longer be allowed.

[392] ACM, ACM starts investigation into Apple's abuse of dominant position with App Store, 11 April 2019.

22 Towards a new blueprint for government automation projects?

Wouter Bronsgeest

The context of the government in the year 2021: an outspoken and diverse society, an extensive government apparatus, many media channels, the call for transparency, accelerating globalisation and new technology. How is the right service provision delivered to citizens in that case? And using what products and services, which are usually largely ICT-based? This poses a real challenge, in particular because these facilities often become available in the form of mobile applications, such as various apps. The coronavirus app is a striking example of this: an app for monitoring and tracking citizens as prompted by coronavirus measures. These kinds of apps are being used in many countries, with varying effect. The apps are part of a broader package of measures that prompted global protests against these measures and the government interference in citizens' personal lives.

Demanding requirements

The most recent speech[393] from the throne expressed the demanding requirements imposed on the government and on government action — and of which the aforementioned protests were partly expressions:[394] (i) on all levels an organisation on which you as citizen can count *and* which provides service on the individual

[393] https://www.rijksoverheid.nl/documenten/toespraken/2020/09/15/troonrede-2020

[394] See examples: NY Assembly Bill A416, and https://www.dw.com/en/coronavirus-german-parents-angry-at-order-to-isolate-their-children/a-54463436. Example of protest in Berlin: https://www.youtube.com/watch?v=oFhuqRDoeXk&feature=youtu.be&fbclid=IwAR2ptkQpB-QlDoeTdRoI4H4Skm51ECYxl0AAxgYPr2xC9jD-cBGammZRQJQ

level;[395] (ii) attention for inclusivity[396] and access and involvement for everyone,[397] (iii) being able to quickly implement new legislation, so being adaptive, flexible and resilient, and (iv) efficient, effective and transparent internal processes and good archiving, also as the basis for accountability.[398]

The use of ICT is becoming increasingly crucial in this. As a result, requirements for creating and subsequently maintaining ICT are also becoming more demanding. The question that arises from this is therefore: Should ICT be made, maintained and implemented in a different way in order to tie in with the requirements stipulated?

(More) successful projects

The time of talking about ICT projects is almost behind us. 'Producing' ICT in projects with an ICT component is increasingly a joint responsibility of the principal, user and IT professional.[399] This also gives rise to more need for cooperation in the chain for creating and then implementing ICT in organisations. The question of whether these projects are being carried out successfully remains an interesting field of research.[400] There is more oversight of projects by, among others, the ICT Testing Office (BIT), the Netherlands Court of Audit and the National Audit Office.

One of the effects of this is that within the government, there is more attention to reducing the size of projects so that they are realisable and realistic parts, improving the likelihood of success. On the other hand, external supervision also results in an abundance of recommendations. These are time-consuming to follow up on and lead to the set-up of more internal control within government organisations. The risk is subsequently that monitoring and reporting get the upper hand. As a result, there is less time to innovate and give experts the room to use their expertise to the maximum.

---

[395] Denhardt, R.B., *Theories of Public Organization*, Thomson Wadsworth, Belmond, California, 5th edition, 2008

[396] https://informatieprofessional.nl/2020/03/knvi-event-2019-in-teken-van-smart-humanity/

[397] Van Deursen, A.J.A.M., Helsper, E.J., Digitale Vaardigheden: een onderzoeks- en beleidsagenda [Digital skills: a research and policy agenda], 20-12-2020

[398] Council of State, Minister responsibility: Unsolicited advice from the advising department, 15-06-2020

[399] Bronsgeest, W.L., Meer vorm dan inhoud [More form than content], Enschede, Gildeprint, 2016

[400] Mulder, H., & Mulder, T., Waarom grote ICT-projecten vaak mislukken [Why big ICT projects often fail]. Informatie, maandblad voor de Informatievoorziening [monthly journal for information provision]. The Hague, Sdu, 2013

Creating differently

Creating ICT increasingly involves new ways of collaborating.[401] This ties in with Rik Maes' plea for working *differently* instead of just giving attention to *more* supervision or *improving* processes.[402] Examples of this include Agile working, DevOps, low-code solutions[403] and the development of apps in cooperation with representatives from the primary process and with users, for instance. It actually concerns working together in multidisciplinary teams, preferably using a production rhythm with short iterations of (portions of) ICT products and services. This poses a challenge because it requires not only expertise but also competence in working together and listening to each other.[404] That is a precondition for working together on solutions that have an impact on the organisation *and* the service provision by the organisation. This way of creating in any event helps to be faster, and consequently flexible and adaptive. It does not, however, yet lay the foundation for also being more resilient;[405] that requires more. Resilience can be achieved by, for example, providing more space for professional development, attention for professionals and experimentation and innovation spaces.

Challenges and preconditions

Although there is already more attention to collaboration and multidisciplinary working in creating ICT solutions, that is not to say that there is already enough

[401] Unhelkar, B., The art of Agile Practice, a composite approach for projects and organisations, CRC Press, Taylor & Francis Group, Auerbach Book, Boca Raton, Florida, 2013

[402] Maes, R., Geen digitale transformatie zonder mentale transformatie: de nieuwe werkelijkheid van de informatieprofessional [No digital transformation without mental transformation: the new reality of the information professional], in: Bronsgeest, W.L., Wesseling, M., Vries, E. de, Maes, R. (ed.), Informatieprofessional 3.0. Strategic skills that keep you connected. AdfoGroup. Amsterdam, 2017

[403] Waszkowski, R., Low-code platform for automating business processes in manufacturing. IFAC-PapersOnLine. 52. 376-381. 10.1016/j.ifacol.2019.10.060, 2019 en https://www.techrepublic.com/article/why-2021-will-be-the-year-of-low-code/

[404] Op de Coul, J., Van Oosterhout, C., Werken in een digitale wereld [Working in a digital world]. Het KNVI Competentie Model: Alles over functies, taken, rollen en competenties [The KNVI Competence Model: Everything about functions, tasks, roles and competences], Van Haren Publishing, Zaltbommel, 2018

[405] Taleb, N.N., Antifragiel, Dingen die baat hebben bij wanorde [Things that benefit from disorder], Uitgeverij Nieuwezijds, Amsterdam, 2020

space for a new way of creating ICT. Aside from the comments already mentioned, there are several other challenges.

The first challenge is in relation to the ICT systems created earlier for the organisation. These were created with reference to the latest insights at the time they were developed. They often form the basis for important parts of the primary process and therefore the *raison d'être* of government organisations. We regard these systems with the knowledge of today as outdated, so-called 'legacy' systems. These systems often support the mechanised version of what used to be manual organisational processes. These systems are, as a rule, based on silos of data and work with a great many interfaces with other systems. With a bit of bad luck, such a system may also have been written with outdated code, and the most recent updates or rationalisation of the system may not have been carried out because this was too low a priority in the ICT portfolio. As such, the precondition for being able to create ICT in a new way is not satisfied. After all, new ICT, creating apps, and making ICT quick and flexible usually assumes a data-centric architecture and a modernised ICT landscape.

The second challenge lies in connecting new ICT products and services to the back office and to relevant (older) systems. Anyone who uses internet banking experiences a direct relationship between making a transfer and receiving funds via the banking app. In actuality, a great deal of extra ICT capacity is deployed on the back-end to process everything in all the banking systems within 24 hours. The ICT products and services of the government face a similar challenge, just of greater scope. It involves many more systems that have a connection with actions that citizens and businesses perform on a website or app. Especially because government organisations are starting to work together more, and exchange data therefore, this challenge is becoming greater.

The third major challenge lies in the area of archiving both policy choices and choices for ICT projects that start up to create government ICT. It must always be possible to trace how choices in the law translate into requirements for primary processes of implementing organisations. And it must subsequently be clear how these processes are supported with ICT. And not only in the here and now, but also with retrospective effect. Seen in terms of time, but also in terms of ICT support versions. In other words, it must be clear what version of the software or app was used to reach a follow-up action or decision on a citizen or business. In supplement to that is the demand for transparency as to how laws are translated into government ICT. That is a complicated issue, especially since political decisions are

the outcome of a negotiation process and cannot always be rationally translated into business rules or logical objective trees.

The next step: three perspectives

In order to arrive at a different way of realising ICT products and services, a number of perspectives for action can be identified for the government.

A first perspective is the creation of products and services together with users in the primary process of the government organisation *and* together with citizens and businesses. Henriëtta Joosten calls this 'encouraging the public sphere'.[406] This still takes place only seldom, and citizens are sometimes actively involved only at the final phase of projects. For example, in testing the user-friendliness of apps. That could be improved. With broader use of multidisciplinary working and extra attention for the professional development of experts in all phases of the production, even more could be achieved.

A second perspective is the collaboration by government organisations in creating products and services, and operating those. Examples are the organising of a central spot for the hosting in a government data centre, the professionalisation of the government cloud, and having apps created or tested by an ICT unit within the government that has a great deal of expertise in this area. This can save money and ensure the optimal use of knowledge. This also gives rise to less dependency on commercial parties, the effects of data gravity[407] can be taken into account and security can be better organised.

A third perspective is the use of new technology. For example, De Nederlandsche Bank[408] published on the use of artificial intelligence for the financial sector, the Customs Authority uses blockchain for supervision of *and* cooperation in logistical processes. There are more such initiatives that can bring about an acceleration in creating new products and services for government organisations themselves, and the service provision to citizens and businesses.

For all three of these perspectives for action, there must be enough latitude in the creation process for evaluating and learning, otherwise we get no further

[406] Joosten, H., De Publieke Sfeer [The Public Sphere], in: Bronsgeest W.L., de Waart, S. (ed.), *Smart Humanity, de mens met 1-0 op voorsprong [Smart Humanity, man with a 1-0 lead],* Hilversum, 2020

[407] https://www.agconnect.nl/artikel/zorgen-van-datacenters-over-data-gravity-door-versneld-thuiswerken (06-05-2020)

[408] Van der Burgt, J., General principles for the use of Artificial Intelligence in the financial sector, De Nederlandsche Bank, Amsterdam, 2019

than isolated initiatives. In a broad sense, evaluating means that there is attention to people, the processes and the products. Attention is also needed for the manner of cooperation and competence development, the way in which attention is devoted to architectures, standards and security, as well as the quality of the end products.

In conclusion

Can the government already take the step towards a different way of creating ICT products and services? And can we already speak of a new blueprint for government automation projects? It is still too early for that. However, government organisations are already on their way. So despite all the amazing technology available, there is no new blueprint. At most, there are the initial contours of a roadmap.

Two analyses

- Apps can be used perfectly well for services that are easy to handle. Offering more complex services via apps, for instance, and embedding these properly in the broader process, including the necessary link to various underlying processes and systems, is a big job. So if the coronavirus app is expanded to include extra functions, that will produce more misery than pleasure on the 'back-end' (and therefore also for the users).

- When creating apps, it is difficult to safeguard the decision making on which the making of an app is based. This includes facilitating accountability in relation to lawfulness and compliance with the law and constitution. Part of this includes straightening out the archiving of data and subsequent decision making performed with the app. This too will be a great challenge for government organisations, and one that will not yet have been implemented everywhere in accordance with the applicable legislation and framework setting. That is unfortunately not much different when it comes to the CoronaMelder app.

23 The government and liability for defective software

Natascha van Duuren and Victor de Pous

If something goes wrong with digitalisation, legal liability can arise, to start with on the part of the supplier. Traditionally this concerned custom computer programs developed in line with the customer's wishes that are delivered with defects, not delivered on time or not delivered at all. Courts in the Netherlands have been considering these kinds of issues since the 1980s, and there is a substantial body of case law for the contractual doctrine of 'failed automation'. While technical problems with computer programs frequently occur, suppliers of defective software and apps are hardly ever sued for this. Certainly not by government organisations. Where do we stand today, seven years after the Elias Commission investigated ICT projects at the central government? One of its recommendations was that lawsuits against defaulting contractors should henceforth be 'the new normal'. What has been done with this recommendation in the intervening period?

Quality

Software code is subject to requirements that can be imposed for the design, programming, configuration, testing, supply, maintenance and, for example, preparation of a roadmap. This also applies for contact-tracing apps ('COVID-19 apps') and other mobile applications. IT professionals make a distinction as a rule. On the one hand, software quality pertains to the functionality; on the other, there is 'software structural quality', i.e. requirements that support the delivery of the functional requirements. From robustness to the degree to which software can be maintained; from efficiency to security.[409] In the event of a defect, special attention is focused on the security aspect of that. After all, insecure computer programs can give third parties access to information systems and therefore to the data

[409] https://en.wikipedia.org/wiki/Software_quality. We leave other quality aspects, such as transparency and 'societal embedding', outside of consideration here.

processed, including personal data and company secrets. And that in turn can result in the placing of ransomware[410] and/or a data leak arising.[411]

In general, you could therefore say that inadequate software security makes individual users, organisations and society more vulnerable than necessary and makes digital crime easier to commit. For our government, the problem prompted the set-up of a new, special form of legal liability for insecure software, or at least this is what emerges from the coalition agreement *Vertrouwen in de toekomst* [Confidence in the future].[412] At the end of 2012, industry organisation Nederland ICT (now NLdigital) placed the blame for the use of insecure software — primarily — on the customer. It is perfectly possible to develop secure software, but if customers do not opt for this, nothing will happen.[413] Five years later, the ECP Platform for the Information Society published an action plan incorporating twenty building blocks. Number 16 reads: "Security in the chain of suppliers is realised by means of a roadmap for secure software. Vulnerabilities in software are fixed through self-regulation and cooperation between users and suppliers."[414] The Rutte III cabinet thought differently in this regard. No self-regulation, but special legislation.

Developments

Although this policy, with significance for society as a whole, has, for reasons unknown, not got beyond the proposal stage, we point to other developments in relation to liability for insecure software code. First of all, the practice. In the best case scenario, after a vulnerability is discovered, the supplier brings out a patch, which the user sometimes needs to install him/herself. This need for the user to install, or rather, the fact that users did not always do so, prompted Minister Grapperhaus (Justice and Security) to express the desire in October 2019 for the

[410] For example, see: https://www.uniklinik-duesseldorf.de/ueber-uns/pressemitteilungen/detail/update-189-it-ausfall-an-der-uniklinik-duesseldorf

[411] Such as experienced by the Medicines Evaluation Board (MEB) and Leeuwarden Medical Centre, among others.
Https://www.security.nl/posting/643318/College+Beoordeling+Geneesmiddelen+slachtoffer+Citrix-aanval

[412] From 10 October 2017.
https://www.tweedekamer.nl/sites/default/files/atoms/files/regeerakkoord20172021.pdf

[413] https://www.security.nl/posting/39339/Nederland+ICT%3A+accepteer+geen+onveilige+software

[414] https://ecp.nl/wp-content/uploads/2017/11/20Bouwstenen.pdf

ability to intervene at companies if the security patch made available by the supplier is not implemented or not implemented quickly enough.[415] This did not get off the ground either.

Also relevant. Following on the serious security leak in the Citrix software — also commonly used by Dutch government organisations and businesses[416] — which was announced in December 2019, the Dutch Safety Board got down to work. In this context, 'special attention was given to the governance of digital security' in the Netherlands, and the Board also included other incidents. "What parties, public and private, have what responsibility and what power to guarantee digital security, and how were these used to limit the effects of this leak?"[417]

In our view, it makes sense that the primary responsibility for — guaranteeing — 'secure' software lies with the supplier, both upon delivery and, in many cases, during a reasonable usage period. But the investigation could lead to other bases for legal liability. The Board will probably follow the line of shared responsibility. In that case, *all* the parties involved — such as the supplier, user and government — bear a duty or obligation of care. With the liability issue, making distinctions can introduce some perspective, in relation to both the defect ('vulnerability level') and the software code: operating system, nature and/or sector of the application, product or service, independent program or embedded.

Elias Commission

We have just determined that the primary responsibility for — guaranteeing — 'secure software' lies with the supplier. What if this party falls short in this respect? And what if a government organisation is the buyer of the software? Has the government found its way to court in the meantime? The Lower House's temporary ICT committee, which carried out the Parliamentary inquiry into ICT projects at the government (the Elias Commission) wrote as follows in Recommendation 34 of its final report. "A contract does not disappear into a drawer after it is signed but is actually used during the project. Lawsuits are becoming normal practice in the event of breach of contract."[418]

---

[415] https://fd.nl/ondernemen/1318504/justitie-wil-ingrijpen-bij-bedrijven-die-digitale-beveiliging-niet-op-orde-hebben

[416] https://support.citrix.com/article/CTX267027

[417] https://www.onderzoeksraad.nl/nl/page/17171/beveiligingslek-citrix

[418] https://www.pianoo.nl/sites/default/files/documents/documents/eindrapportgripopict-oktober2014.pdf

The policy proposal from the Rutte III cabinet for the introduction of special legal liability for insecure software in Dutch law — possibly via a new type of risk liability instead of liability based on fault (culpable behaviour) — gives the impression that the current liability law is not functioning adequately or at least does not sufficiently enforce secure computer programs. The question is whether the introduction of a special liability means that a government organisation will take an ICT supplier to court if it delivers defective software, with the cited recommendation from the commission in mind. Or will the government remain extremely reticent to bring lawsuits or alternative forms of dispute settlement, such as arbitration, binding advice and mediation?

Bark but no bite

The public legal database www.rechtspraak.nl gives access to four civil cases that we can qualify as ICT disputes in which the government was a litigant.[419] Two of the four cases involved a case brought by the ICT supplier against the government. Two other cases remain in which a government organisation sued the ICT supplier. The first involved proceedings against an individual IT professional who reportedly acted negligently in conducting a tendering procedure,[420] and the second pertains to a claim for performance in summary proceedings against IT service provider Centric, in which the plaintiff demanded performance of the agreed ICT service provision.[421] Not an impressive score.

Could it be the case that ICT projects are now going so smoothly at government organisations that there is no need to take matters to court? This explanation is not very convincing, however. One example. In 2017, Minister Plasterk (Home Affairs and Kingdom Relations) put a stop to the BRP project (Key Register of Persons) after almost ten years of development. Many tens of millions of euros had already been spent on the project.[422] Two years later, Minister Schouten (Agriculture, Nature and Food Quality) pulled the plug on a large computerisation project for regulatory body the Netherlands Food and Consumer

[419] Also see J. van Helden, Schikken of procederen? [Settle or litigate?], AG Connect November 2020.

[420] ECLI:NL:RBROT:2016:4318

[421] ECLI:NL:RBNNE:2018:484

[422] https://nos.nl/artikel/2181664-plasterk-stopt-met-geldverslindende-vernieuwing-bevolkingsregister.html. Also see: https://www.rijksoverheid.nl/actueel/nieuws/2018/05/18/lessen-trekken-uit-operatie-basisregistratie-personen for the lessons that should be learned from this.)

Product Safety Authority (NVWA), after the ICT Testing Office (BIT) had advised that the project be stopped. More than €65 million had already been spent on this.[423]

Less value for money?

The government must guard against getting less value for its money than commercial customers. What do we mean by that? As soon as ICT suppliers have the impression that the government will not take (legal) steps anyway — even if a supplier does not comply with its obligations — there is a good chance that the supplier will set the bar somewhat lower when performing the contract. This can manifest, for instance, in responding less adequately to issues that go wrong and to escalations by the government. The government will, since it usually does not proceed to take further legal steps, try to salvage the project by approving the change and contract variance requests. The result of this is that the parties muddle on, sometimes for years, the execution of the project ends up further from the original agreements and the (additional) costs rise even higher.

Another possible consequence is that tenderers in a tendering procedure prescribed under European law[424] will be more inclined to make promises of which they know in advance they will probably not be able to fulfil them. Their interest in doing this is obvious. By submitting such a tender, the suppliers increase the likelihood they will win the contract. These usually involve very large projects, so there is a large financial interest in landing a government contract. It is plausible that suppliers will consider the risks involved with submitting such a tender to be minimal. After all, they know that if push comes to shove, the government usually does not proceed to take legal action. So the likelihood that suppliers will be sued is small. In most cases, the government opts to continue the project with the same supplier. As a result, the government does not get what it had in mind when putting out the tender. In other words, less value for its money.

Conclusions

There is no doubt that computer programs with defects, including security defects, make buyers (the customers) more vulnerable than necessary and can easily result in damage. This fully applies for mobile applications. Added to this is the fact that if a government organisation is faced with defects in (third-party) software, this can

[423] https://www.rijksoverheid.nl/actueel/nieuws/2019/04/15/minister-carola-schouten-stopt-implementatie-en-ontwikkeling-ict-systeem-inspect-bij-nvwa

[424] See chapter 6.

virtually immediately cause effects for — part of — society. It follows from the Rutte III cabinet's policy proposal to introduce special liability for insecure computer programs in Dutch law that on the government level in any event, the importance of secure software is recognised; but only on paper, because this proposal has not been implemented.

What a rapidly digitalising society needs is software and other digital technology with a good mark for *all sorts* of quality aspects, whether or not these are delivered by a traditional software company or the application has been developed in-house by the organisation, no matter the sector. The next question — whether achieving sufficient digital quality requires new legislation — is less opportune for the government as a customer to that extent than for the business sector. This is because based on its own purchasing terms and conditions, the legal position of government organisations is stronger than that of businesses in similar situations. That makes it all the stranger that in the event of breach of contract, government organisations do not stand up for their interests, or at least not strongly enough. Taking stock of the situation seven years after the Elias Commission, one can only conclude that government organisations have a lot of bark but no bite, even though they do have teeth.

Points in conclusion

- In a society that has become virtually entirely dependent on automated data processing, the importance of good software quality is only increasing. Moreover, the vulnerability of society increases the moment the government purchases insecure software.

- At the point that a government organisation ascertains that the software it has purchased does not function properly and/or is insecure, it must take steps against the supplier. According to the Elias Commission, lawsuits should become the norm in the event of breach of contract. Seven years later, this 'new normal' has not materialised, but conflicts can also be approached otherwise.

- In our view, the crux is a change in frame of mind; a different fundamental attitude. Government organisations must act more professional and business-like when dealing with problems with digital suppliers. That is not only of societal importance, as ICT has been a prerequisite for every government

organisation for years already, but also brings benefits for the digital sector. After all, the parties need each other. The government leans heavily on external suppliers in order to realise policy; the public service sector is an important client for the digital sector. Ultimately, both therefore benefit from a mutually mature, expert and business-like attitude.

24 The Integrated Information Support System for Infectious Disease Management of Korea

Jee-In Kim

ICT can be utilized to overcome the COVID-19 crisis. The Korean government enhanced the infectious disease management system by actively using ICT. There are four stages of the strategy to respond the COVID-19 crisis in Korea. The first stage relates to 'Screening and Diagnosis' to identify patients and separate them from the public, while the seconds concerns 'Epidemiological Investigation' to precisely identify recent travels of people confirmed with the disease and track their activities. Accordingly, the third stage focusses on 'Patient and Contact Management' to manage hospital wards and prepare for the shortage. The final stage focuses on 'Prevention', in order to limit the spread of infection by opening public data. Though there are serious issues of violating privacy and restricting freedom of people, the Korean government could successfully form social consensus by communicating people based on the failures of the past.

Introduction

The Republic of Korea utilizes ICT (Information and Communication Technology) to overcome the COVID-19 crisis. The integrated information support system is developed as the main tool. The goal is to control the disease by tracing, monitoring and managing patients and people that tested positive to the disease, while quickly providing information by opening public data to deal with the crisis. There are four stages of the ICT based strategy to respond the COVID-19 crisis in Korea:

1. 'Screening and Diagnosis' to identify COVID-19 patients.
2. 'Epidemiological Investigation' to identify travels of people confirmed with COVID-19 and track their activities
3. 'Patient and Contact Management' to manage hospital wards and prepare for the shortage

4. 'Prevention' to limit the spread of infection by opening public data

The four stages, briefly described hereunder, explain how the Korean government enforces the strategy.[425]

Stage 1: Screening and Diagnosis

National Quarantine System
The quarantine system shares and uses data and ICT systems as follows:

- Receives entrants' data from airlines and telecommunication companies
- Screens entrants from affected countries and sends their data to Ministry of Foreign Affairs (MOFA) and Ministry of Justice (MOJ).
- Collects additional data of entrants from MOFA and MOJ.
- Sends text messages to entrants from affected countries and provides their data to Health Insurance Review & Assessment Service (HIRA) and National Health Insurance Eligibility Verification System (NHIS).
- Shares the data with medical institutions via information systems of HIRA and NHIS.

Walk-Through Screening Center
A COVID-19 walk-through screening station is a one-person walk-through screening booth. The booth is about the size of a public phone booth. It consists of durable transparent resin plates, with two openings in the booth for gloves to be attached for healthcare professionals to interact with the test subjects. The healthcare professionals examine the subject's symptoms using a two-way speaker phone. The examination itself is normally completed within one minute, but with another 5 minutes needed to disinfect the screening area. It means that about 10 test subjects can be screened per hour.

[425] It is a summary and paraphrase of a report titled 'Korean ICT services against COVID-19 pandemic' published by National Information Society Agency (NIA) of Korea https://eng.nia.or.kr/site/nia_eng/ex/bbs/View.do;JSESSIONID=C10E7B3D6DF6789E9D179BD67DF0DB86.ea66bd9e7dd806361559?cbIdx=31975&bcIdx=22150&parentSeq=22150

Drive-Through Screening Center

The Drive-Through screening method focuses on increasing the efficiency of sample collection and reducing the risk of cross-infection between subjects and healthcare professionals. It minimizes the screening and disinfection areas, as compared to the screening stations installed and operated to cope with the Middle East respiratory syndrome coronavirus (MERS) in 2015. It took 30 minutes for a single subject screening case in 2015 to deal with MERS. Now, the Drive-Through method can handle each screening case within 10 minutes.

Stage 2: Epidemiological Investigation

The Epidemiological Investigation System automates the process of contact tracing for COVID-19 confirmed patients. Geospatial information on the travel routes of confirmed COVID-19 patients can be visualized on a map. It also provides related statistical information. An analysis tool called 'City Data Hub' is used to collect and process large-scale city data sets. Once a patient is confirmed, Korean Centers for Disease Control and Prevention (KCDC) requests contact tracing related information. The requested information is provided after obtaining the consent for utilization of personal information from the police and the Credit Finance Association of Korea. Domestic mobile service providers and credit card companies provide the personal information of the confirmed patients based on police approval. The system provides the result of analyzed data of the travel routes of confirmed patients and hotspots by processing and analyzing the information. There are a couple of serious issues about developing and operating the system:

- Legal basis for sharing personal information for emergency response: as the investigation provides personal information to the public, strict measures for privacy protection must be followed. Utilizing personal information from confirmed patients is based on a law (Infectious Disease Control and Prevention Act) that has been revised after the so-called MERS outbreak in 2015.
- Close communication and cooperation with the private sector: patient monitoring is especially challenging if people infected with the virus hide information or lie during the investigation. The telecommunication companies in Korea provided information for contact tracing.

Korea could develop the epidemiological investigation system by revising the law and cooperating closely with the private sector. It cannot be executed easily in Korea without the previous painful experiences of the MERS outbreak in 2015.

Self-Quarantine Safety Protection App

A mobile app called 'Self-Quarantine Safety Protection App' was developed to monitor people under self-quarantine. This app supports both the citizens under self-quarantine (as users) and assigned government case officers (as managers). A user checks her/his health status twice a day with the app, and the results are automatically delivered to the assigned case officer. The information about the location is managed. If the user leaves the quarantine area, a notification is sent to the user and the officer, allowing the officer to respond and handle the situation immediately.

Negative Pressure Isolation Room Information System (NPIRI)

A negative pressure isolation room is an isolation chamber with ventilator, air-conditioning system, and open space corridor that generate and maintain negative pressure to prevent airborne infection. It is essential to treat severe COVID-19 patients. The operational status data management system was developed to promptly and efficiently allocate severe COVID-19 patients to the negative pressure rooms. The system allows monitoring on the status of negative pressure isolation room operation at medical institutions across the country. The system provides data on the use of negative pressure isolation rooms by COVID-19 patients each day, allowing the government to monitor and manage the units effectively.

Stage 3: Patient Management Information System (PMI)

The Patient Management Information System is designed to systematically manage COVID-19 patients to prevent further spread and check their real-time status. KCDC, local quarantine task forces of cities and provinces, public health centers, community treatment centers and medical institutions can manage information on allocating of confirmed patients to monitoring organizations, patient conditions, hospitalization or transfer, isolation or release, and deaths.

Stage 4: Prevention

Open public data on COVID-19

A face mask is considered as an essential tool to prevent the COVID-19 virus from spreading via people. Disclosing information on face masks distributed by the government to the public as open data is considered as a good example of opening of public data to prevent the spread of COVID-19. Based on the open data, developers in the private sector in Korea released over 150 apps and web services. Such apps and services showed a high usage rate by recording 670 million API calls on face mask in 3 weeks. People were able to check the remaining inventories of face masks in nearby pharmacies and markets easily and buy them.

Pathogens Information Management System (PIMS)

The National Culture Collection for Pathogens (NCCP) has established the Pathogens Information Management System (PIMS) in 2010. The main features of PIMS include registration of pathogen resources information, management of location and storage facility information, information on quality management, deliberation and management of pathogen resource registry, management of online and offline distribution, and management of statistical data. PIMS provides services including search of pathogen resources and management of distribution, deposit, outbound transfer and approval of acquisition of pathogen by foreign and international institutes based on pathogens resource database of specialized banks and NCCP.

Concluding Remarks

The Korean government enforced an extremely strong policy to overcome the COVID-19 crisis by revising laws and utilizing ICT. Though it seemed to work, it caused serious legal and ethical issues such as violating privacy and restricting freedom of people. In the past, the government failed to control epidemic diseases effectively such as the Ebola virus disease in 2014, MERS-CoV in 2015 and Zika virus disease in 2016. Such failures in controlling the diseases were one of important reasons why the current regime could take a political power in 2017.

The Korean government continuously enhanced the infectious management system by revising laws and adopting ICT. The lesson from the previous failures also includes importance of information sharing with stakeholders, communication with citizens and promotion of government policy to public. The

government could effectively form social consensus by reminding people of previous failures in controlling the epidemic diseases.

As of 13 January 2021, the number of confirmed cases in Korea is 70,212 and the number of deaths amounts to 1,185. The numbers may not look extremely disastrous comparing to others in the world. However, there remains a long way to control the disease. It is not certain how long the people of Korea could stay being cooperative to the government policy as the restrictions on freedom, privacy and economy continue to affect them. Hopefully, valid vaccines and remedies for COVID-19 can resolve the problem as soon as possible.

25 The importance of supervision on mobile applications

Maarten Souw

With reference to one case study, we explore the possibilities that an IT auditor has in assessing the functioning of apps. This concerns the CoronaMelder contact-tracing app from the Ministry of Public Health, Welfare and Sport, which has been generally available since 10 October 2020. The COVID-19 app is suitable for that because the department deliberately made all the information necessary in this context publicly available. Based on the case study, points for attention for the auditor have been derived and summarised. As emerges from the case study, the assessment of apps confronts the digital auditor with interesting choices. Will he focus on an in-depth assessment of the app, the environment in which the app operates, or does he want to bring the different parties together? In this relatively new playing field, the IT auditor can also demonstrate his added value by means of a good risk assessment.

Context

Mobile applications, often called apps for short, are increasingly replacing traditional applications. Moreover, apps are constantly developing into new networks of services. The fact that apps play an increasingly determinative role in an (IT) ecosystem is due to a number of reasons, in our view. Of all the information systems, apps are the closest to the end users; their user experience largely determines the customer perception. Apps are also usually small and, as such, quick to build.

The financial world is a good example. Sending a friend a request to pay you back and investing via the mobile phone have become commonplace, but we are just at the beginning of the development. For instance, the European PSD2

Directive[426] brings combined sales and payment apps a step closer by. After all, with this directive the EU envisions promoting innovation and competition in the area of payment services. Looking at this trend more generally, even smarter and more innovative combinations are imminent; apps that are laid like a blanket over all sorts of competing market parties and their service provision. Every reason to devote some attention to the ways in which an IT auditor can assess an app in its context, therefore.

Assessment of (small) systems

Roughly two approaches are commonly used in assessing an IV solution — the traditional work area of an IT auditor:

1. A process-based opinion, also called 'around the application'. The IT auditor in that case assesses whether the design, development, test and management process have functioned adequately. He uses this to form an opinion as to to what extent an application will behave in accordance with the specifications; the limitation of this working method is that an application is seldom tested for unintended use or behaviour.
2. A technical assessment of the IV solution, also referred to as 'through the app'. Here the IT auditor studies the behaviour of the system and/or verifies the source code. This enables the IT auditor to investigate whether the behaviour of the IV solution matches the desired functionality and whether the software satisfies the usual quality standards. This could include, for instance, testing the OWASP vulnerabilities in order to be able to quickly locate and close any gaps. It will also at least be determined in this context whether the software does not make more possible than was intended.

CoronaMelder

The Dutch contact-tracing app the CoronaMelder constitutes part of the public health strategy of testing, warning and self-isolation. The idea is that people who have tested positive can anonymously and quickly warn the other people to whom they have been in proximity; the people who receive a warning can in turn have themselves tested or self-isolate. The first version prompted a public debate

426 Payment Services Directive (EU) 2015/2366, European Parliament and the Council of 25 November 2015.

because of the risk of breach of privacy and/or freedoms.[427] This call translated into, among other things, debates in the Lower House of Parliament and — one of the ultimate outcomes — the formulation of ethical guidelines.[428] This on account of the risk of breach of privacy and freedoms.

The discussion also resulted in a transparent working method for the ultimate CoronaMelder app. Discussions in the Lower House of Parliament are, naturally, minuted and publicly searchable. The second way in which the wish for a public debate has been complied with can be found in the safeguards in relation to the (privacy) rights of the users. The use of the CoronaMelder app is voluntary, and the app deals with the user's privacy carefully; the application only exchanges an anonymous key, and only the end user knows the key corresponds to it.

The open-source approach was used to develop the app so that more people could be given insight into the functioning of the app. The source code and designs were published each time on the Github platform, a public source for open-source software code.

The environment and the app were also tested carefully and in the traditional manner. The back-end and hosting of the app were also subject to penetration testing by NFIR[429] and Fox-IT. These results were published; a form of transparency that is not often seen.

Conclusions

Three things stand out in our study. First of all, the requirements from the ethical framework, in this case the privacy conditions, have been demonstrably incorporated in the definitive product. It also emerges to be possible in this case to make the connection between the user requirements and the app delivered. However, more than in the 'waterfall' era of the past, the assessor does have to make these connections himself; after all, the traditional phases such as functional design and technical design often blend with each other in app development.

---

[427] The open letter of 13 April to the ministers involved. 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, retrieval date 22 January 2021

[428] See dossier 25952 in the documents of the Lower House, in particular number 240: the letter from Minister De Jonge about the CoronaMelder. (kamerstukken.nl)

[429] Report on Penetration Test, project name 20063 Cholet, IT Forensic and Incident Response, 1 September 2020.

In addition, the software review highlighted issues that would perhaps not have been noticed in a purely process-based approach. The Dutch COVID-19 app emerged to use an older software library, for instance. The app also does not check whether the underlying operating system is 'rooted'.[430] A user can break through the security on his smartphone ('jailbreaking' or 'rooting'). This gives the user more flexibility but often leads to weaker security of the smartphone. These findings were not considered to be blocking for the use of the CoronaMelder; it does illustrate the added value of this approach. They show that the observation 'the software does it by itself' can leave weaknesses unnoticed.

Finally, it also emerged with the CoronaMelder that a chain is only as strong as its weakest link. The person using this app must, where this is appropriate, request a test. The requesting, scheduling and viewing of the tests also takes place on computer systems. It is precisely in these later process steps that the security did not produce the desired result.[431] [432]

Points for attention

Experiences in relation to the CoronaMelder app have produced good insights. If we generalise these, we see three main risks that the IT auditor must take into account in connection with each other. These are (i) preconditions, (ii) the development process and (iii) context of use.

(i) Preconditions for app development

Not every app has as extensive a body of stakeholders and ground rules as the CoronaMelder. Nonetheless, apps are often part of a network of services that reach across different sectors or countries — and their legislation and regulations. It will often not be feasible to have sufficient knowledge of all sectoral regulations. In this case, the app builder's (compliance) policy can offer a solution. Ideally, such a policy would take into account the essential legislation and regulations. The same consideration applies for stakeholder management. If the app builder's policy has been adequately attuned to this, the IT auditor can limit himself to how the end user is dealt with. Of course, he must consider engaging an external expert if this policy is lacking or not sufficiently implemented.

[430] Source Code Review, Brucker et al., Secura 19 August 2020

[431] Verhagen, Modderkolk, Datalek GGD [Data leak at GGD], Volkskrant, 28 January 2021

[432] GHOR response to report from DigID, GHOR, 10 February 2021

(ii) Development process

Assessing this requirement has been part of the auditing profession for some time already. As far as the assessment of software acquisition (in this case, building) is concerned, the profession has various reference points. For a somewhat more traditional world, the Plan (APO) and Build (API) phase of CObIT [433]can serve as a good starting point. For the somewhat more flexible agile working methods, the IT auditor can delve into common working methods such as Scrum;[434] this popular (agile) way of working involves various reference points, such as policy documents, product mapping and the 'definition of done'. The auditor can determine whether the requirements in these artefacts tie in with the company's policy. Does the IT auditor see sufficient attention to the compliance requirements and that the product owner has carefully weighed the different user wishes? And he must also investigate whether the software has also been adequately tested in the agile working method.

In addition to this process-based control, the case study also goes into penetration testing and software review. We regard these techniques as a supplement to the process-based assessment for two reasons. The first reason is that while a process-based assessment may produce the necessary certainty about the software quality, the actual behaviour of the application can only be assessed with reference to the application itself.

The second reason is that not every IT auditor has the expertise or resources to assess software code or carry out a penetration test — and these will not always be applied, therefore. Software assessment cannot therefore be seen as a substitute for a processed-based assessment, or vice versa.

(iii) Context of use

'Jailbreaking' or the use of an app more generally is, of course, the responsibility of the end user. Nonetheless, the IT auditor can, in his opinion, still take into account the interests of the end user. The general terms and conditions or communication with the end user are the reference points in this. The IT auditor can look into whether the customer has been alerted to the risks and responsibilities in the use of the app.

---

[433] Control Objectives for IT, https://www.isaca.org/resources/cobit, retrieval date 18 February 2021

[434] Scrum is a popular form of agile working. Information can be found at www.scrum.org or https://agilemanifesto.org/

The IT auditor must also consider how to deal with risks in the surrounding infrastructure. These risks are not necessarily picked up in an assessment of software or a computer centre. The IT auditor often leaves these kinds of environmental factors out of his audit; in the assessment of apps, we do consider a more active role to be appropriate. The ecosystem plays a decisive role in the ultimate security and functioning of the app. The IT auditor can make the principal aware of these risks. For instance, he can point out the possibilities of perhaps 'isolating' the app more on the end user's device.

Conclusion

The CoronaMelder app illustrates the dilemmas with which the IT auditor wrestles. How much attention does he devote to a thorough investigation of the app and how much attention does the context of the app require? The Dutch contact-tracing app demonstrates the added value of a good assessment in advance but also illustrates that the inspection cannot be a one-off or too limited in scope. Somewhere the need for a single overarching regulator is taking shape, but pending that, the IT auditor can be expected to temporarily fulfil this role in any event. With this in mind, we reach three recommendations:

- challenge the principal to see the audit domain as being broader than the app or the company's direct interests alone;
- assess all the security measures present (and possibly missing) in cohesion with each other;
- in the absence of a single overarching oversight body, make contact with the relevant competent regulators or experts.

26. Ethics and Contact Tracing Apps: A Better Way Forward?

David Kreps and Liesbeth Ruoff-van Welzen

App-based COVID-19 contact tracing systems have proved very controversial in many countries, with constant new developments, and notable national differences in project approach and deployment. What insights can we gain from these experiences? In this chapter, we look at three app-developments in different countries, and ask: where do we stand with regard to digital quality? By digital quality we mean the security aspects, IT architecture, liability for defective computer programs, privacy protection in practice, governance of IT projects, the ethical side of digitization, the understanding of open-source software, the freedom to choose an application, the financial aspects of data processing, auditing digital systems and, for example, our dependence on Big Tech? Where or how, specifically, does an ICT professional stand on these and related issues? Can an ethical code provide a helping hand?

Contact tracing apps

We start our journey in France. In this country the centralised eGovernment solution taken by the government failed because the 'digital-first' approach - when digital artefacts are created to represent reality before reality is known – often misses vital details, and frequently alienates most stakeholders. The relevant experts, moreover, were simply not consulted in the rush to create a solution from an incomplete understanding of the phenomenon. Any smartphone solution needed to be "discussed and designed for transparency and trustworthiness," but instead the French Stop-COVID app that was initially – and hurriedly - created included "inadequate specifications and *irrelevant* data collection".[435]

In the Netherlands the COVID-19 governmental taskforce had the impression that they could adjust an existing App to this new Corona situation.

[435] Rowe, F., Ngwenyama, O., & Richet, J. (2020) Contact- tracing apps and alienation in the age of COVID-19, *European Journal of Information Systems*, DOI: 0.1080/0960085X.2020.1803155

They sent out the question, with answers requested in two weeks' time. 700 offers were received of which there were 660 real proposals. 7 of these were invited for a presentation of their prototype during the weekend of 18-19 April 2020 to a mixed group of experts and users. The result was a NO GO. The government then decided to build the app itself.[436] That process was finalised with the roll-out of 10 October 2020.[437]

'World-beating' technology

Meanwhile in the UK, in the Spring of 2020, the Ada Lovelace Institute published a searing report, telling a government that was lauding the 'world-beating' technology solution it was planning to roll-out, that "There is an absence of evidence to support the immediate national deployment of the technical solutions under consideration" and that "Until a robust and credible means of immunity testing is developed, focus should be on developing a comprehensive strategy around immunity that considers the deep societal implications of any immunity certification regime, rather than on developing digital immunity certificates."[438]

It added, for technology providers and developers, that "the rushed deployment of technical solutions without credible supporting evidence and independent oversight may undermine public trust and impede the effectiveness of the implementations in supporting the crisis response". In fact, the original app was abandoned as not fit for purpose – and clearly far from 'world-beating'.

Building trust

An appreciation of how best to approach sensitive and large-scale ICT projects such as the COVID-19 apps, both amongst the profession and those in government commissioning such work, could have prevented much wasted time, effort, and money. The IFIP Code of Ethics might have been useful during 2020! In September 2020 on Zoom the IFIP General Assembly enthusiastically adopted a new IFIP Code of Ethics and Professional Conduct.[439] IFIP is The International Federation for Information Processing, a UNESCO affiliated NGO, and the leading multinational,

[436] https://www.rijksoverheid.nl/actueel/nieuws/2020/04/17/zeven-apps-doen-mee-aan-publieke-test-komend-weekend

[437] https://www.rijksoverheid.nl/actueel/nieuws/2020/10/10/landelijke-campagne-van-start-voor-wie-download-jij-coronamelder

[438] Ada Lovelace Institute (2020) *Exit through the App Store?* www.adalovelaceinstitute.org

[439] https://www.ipthree.org/ifip-code-of-ethics/

apolitical organization in Information & Communications Technologies and Sciences.[440] This is a very welcome international development, in a field where there is a dizzying array of sometimes rather questionable codes (or none at all), with the result that all too often none is adopted or followed. Without appropriate standards, ICT professionals can find themselves contributing to public harm.

The public harm to which ICT professionals are currently contributing is well documented – one need think only of the scandals around Cambridge Analytica, the facial recognition app Clearview AI, and the epidemic of covert web tracking. Not to mention software in Boeing airplanes or Volkswagen exhaust tests. Most ICT practitioners are well-intentioned individuals, but the normal ethical insights of well-intentioned individuals are stretched by the ways that new technologies impact society, as these examples illustrate. Ethics, importantly, is a matter of professionalism, outside the purview of law and regulation. A Code of Ethics, therefore, does the heavy lifting of providing a well-thought through guide for well-intentioned individuals to follow.[441] Perhaps the most important outcome of the application of an ethical code within a profession is development of *trust*, by the public, in that profession, and what those professionals provide. A Code of Ethics – like the Hippocratic Oath in the medical profession – enables the public to be reassured that those within the profession have the public good at heart.

Accepted

The new IFIP Code has been adapted from the ACM Code of Ethics[442] published previously, which itself had been developed through many years of consultation and development with members of IFIP, IEEE, other national and international bodies and companies – including KNVI - and was published in 2019. An IFIP Code of Ethics Task & Finish Group set up at the IFIP General Assembly in Kiev, Ukraine

[440] www.ifip.org. Every year the IFIP General Assembly (GA) gathers for its annual meeting. The Dutch Royal Society of Information Professionals, KNVI, is the Dutch representative. The GA includes representatives of National Computing Societies from over thirty countries around the world, plus 'members at large' including the ACM, and the Chairs of the 13 Technical Committees (TCs) who represent literally thousands of academics and practitioners, from all over the world, focussed on research work around multiple different aspects of ICT.

[441] Gotterbarn, D., Kreps, D. Being a data professional: give voice to value in a data driven society. *AI Ethics* (2020). https://doi.org/10.1007/s43681-020-00027-y

[442] https://www.acm.org/diversity-inclusion/code-of-ethics

in September 2019, then undertook further consultations with Member Societies and with the IFIP Board, to produce the final version adopted at GA2020.

The IFIP Code of Ethics is not intended to replace Codes specific to Member Societies, which may contain unique points relevant to their cultures. The Code contains elements, however, that might not be included in the Member Society Code. Therefore, the IFIP Code of Ethics can be adopted alongside a Member Society's Code, or Member Societies can modify their Code to include those values and guidance not already included in their own Codes or simply reference it in addition to their own codes.

Four domains

The IFIP Code is broken down into four sections: General Ethical Principles; Professional Responsibilities; Professional Leadership Principles; and Compliance with The Code. In the past, some Codes of Ethics contained specific imperatives or benchmarks. Codes with fixed benchmarks, however, in our rapidly changing ICT environment, are rapidly outdated, and do not help ICT practitioners make proactive decisions in complex situations. The IFIP Code provides aspirational guidance that can accommodate a rapidly changing profession. Thus, the first section contains seven common ethical principles consistent with all professional codes. Section 2 provides nine specific ICT professional responsibilities in the light of the general principles of section 1. Section 3 adds seven responsibilities to ICT professionals when they have leadership responsibilities. Last – and least – two of the 25 principles deal with compliance, advocating proactive support for the rest of the principles.

How ethics could have saved us all the trouble

The IFIP Code has achieved something rare and quite precious – international consensus. In the words of Jussi Nissilä, CEO of the Finnish Information Processing Society (TIVIA) the IFIP "code has been gone through, line-by-line, by the TIVIA Working Group on Ethics, and no reason to not adopt it was found – on the contrary, the Working Group on Ethics considered it to be culture independent, and suitable for TIVIA, as well as any computing society".

Maxine Leslie, Secretariat and Committee Manager at the British Computer Society, also reported that "The BCS Academy of Computing has reviewed the proposed IFIP Code of Ethics and will be pleased to endorse it, finding it a very

robust document covering a variety of important and interesting topics."[443] Vicki Hanson, CEO of the ACM, said "As an international member of IFIP, ACM endorses the proposed IFIP Code of Ethics as a common international standard for computing and the profession."[444]

Leadership, understanding, and the ethical skills to avoid the problems that arose - especially in building up the public trust necessary for the successful roll-out of these coronavirus apps - could all have benefited from the IFIP Code of Ethics. Thankfully, it will finally be published in 2021 and it is to be hoped that the uptake all over the world will be enthusiastic and impactful.

Conclusion

Public Trust is essential to the roll out of major ICT innovations, particularly in the arena of public health. Ministerial ignorance and corporate overpromising squandered the possibilities that could have been realised from ICT engagement in the fight against the pandemic. First and foremost, informed leadership is needed. This is explicitly part of the Code: Professional Leadership Principles. Thereafter, the Code could have helped *police* the process, ensuring that those ICT practitioners who did become involved, were appropriately guided by principles that would engender the public trust that any such sensitive ICT application required (Professional Responsibilities). Finally let us not forget the importance of the General Ethical Principles, which should form a condition of every digital process.

Points of relevance

- Ethics is a matter of professionalism.
- Laws and regulations are created based on a society's ethics, to enforce behaviours we are expected to follow, but ethics suggest what we *ought* to follow, and help us explore options to improve our decision-making.
- The IFIP Code of Ethics seeks to provide an aspirational set of principles for what ICT practitioners *ought* to do.

[443] Email to David Kreps from Maxine Leslie.

[444] Email to David Kreps from Vicki Hanson.

- The IFIP Code of Ethics is a common international standard for computing and the profession.

- Ethical Leadership in ICT is as important as Ethical Behaviour among Practitioners.

List of authors

- Dr. J. Baaijens is a Senior Research Fellow at the Department of Organisational Sciences at the University of Tilburg.
- Dr. M.J.K. van de Berg is a researcher (research group Artificial Intelligence) and teacher and supervisor of master students at the master of Informatics at the University of Applied Sciences in Utrecht.
- Professor dr. E. Beulen is full professor at Tilburg University and Academic Director for the executive MSc Information Management & Digital Transformations at TIAS School for Business.
- Drs. J.M. Bommeljé is information architect, database designer and programmer.
- Drs. K. Brongers is partner at Bureau for Management & ICT (BvMI) and member of the Advisory Board of the KNVI.
- Dr. W.L. Bronsgeest is Head of the Directorate Support Office, Management Team Directorate IV Tax Authorities, Ministry of Finance and duo chairman of KNVI.
- L. Dohmen RI works as a consultant at KEMBIT and is chair of the KNVI Special Interest Group Research and Education.
- N.H.A. van Duuren is attorney-at-law partner for IT, IP & Privacy at De Clercq Lawyers and Notary in Leiden/The Hague and chair of the KNVI Special Interest Group IT and Law.
- J. van Helden is attorney-at-law for IT, IP & Privacy at De Clercq Lawyers and Notary in Leiden/The Hague and member of the KNVI Special Interest Group IT and Law.
- Dr. Jee-In Kim is a Professor at the Faculty of Computer Science and Engineering at the Konkuk University, Seoul, Korea.
- Dr. C. Juiz is Full Professor Computer Architecture and Technology at the University of the Balearic Islands, Spain.
- Dr. P. Kotzé is Extraordinary Professor at the Department of Informatics of the University of Pretoria, South Africa.
- Dr. D. Kreps, (NUI Galway), Chair IFIP Code of Ethics Task and Finish Group (http://david.kreps.org/).
- Mr. R. Ludding is attorney-at-law for European and Competition law at De Clercq Lawyers and Notary in Leiden/The Hague.
- Professor Dr. R. Malaka is head of the Digital Media Lab at TZI, University of Bremen.

- Mr. ir. L.H.A. Morsink is senior business architect at business/IT consultancy company Dekker, Morsink & Partners which he also owns.
- P.W.M. Oor CISSP CCSP CISM CIPP/e is Chief Security Officer at Conclusion and is member (former chair) of MSP-ISAC-NL.
- Dr. S. van Otterloo is a consultant on software development, privacy and AI at the ICT Institute.
- V.A. de Pous is an independent IT lawyer and analyst in Amsterdam and co-founder and board member of the KNVI Special Interest Group IT and Law.
- Professor Dr. K. Rannenberg is Chair of Mobile Business & Multilateral Security, Goethe University Frankfurt.
- L. Ruoff-Van Welzen is chair of the KNVI Special Interest Group Digital Skills, member of CEN TC 428 IT Professionalism and Digital Skills, Director IP3 (IFIP) and director of LRWA in Voorburg.
- Drs. G. Speijer is radiation oncologist at the Haga Hospital and founder of the care innovation company CatalyzIT.
- H.L. Souw RE CIPP/E is Information Security Officer at The Dutch Authority for the Financial Markets in Amsterdam and chair of the KNVI Special Interest Group IT Audit and Risk.
- Mr. S. Wallagh is training manager HBO-ICT Cyber Security & Cloud, Technical Informatics at the University of Applied Sciences in Utrecht and board member of the KNVI Interest Group IT and Law..
- Mr. M. de Wijs is attorney-at-law for IT-procurement law at De Clercq Lawyers and Notary in Leiden/The Hague.
- Dr. D. de Wit CMC is adviser at Bvolve in Zeist, chair of the KNVI Special Interest Group eHealth and involved in the Digital Skills in the Healthcare Sector coalition.
- A. Wong FACS is Managing Director of AGW Consulting Pty Ltd, a multidisciplinary legal and advisory practice in Sydney, Australia and Vice President of IFIP.

Digitalisation plays an important role in combating the SARS-CoV-2 coronavirus. Information systems collect tests, analyse data on spread, simulate infection risks or register vaccinations. Mobile applications with diverse objectives offer different functionalities, sometimes on the basis of artificial intelligence. At the same time, general information technology lends a helping hand. We work, operate and spend remotely en masse. From a legal perspective, the right to privacy carries a great deal of weight in healthcare. Europe has a stricter data-processing regime for special personal data, including information about our health, for instance.

Especially in response to contact-tracing applications (COVID-19 apps) — for the purposes of an automated identification and warning system for people who may have been in contact with an infected person — dilemmas, choices and controversies arise each time; and not only in relation to the protection of our privacy. This book seizes on these diverse events and national differences to obtain insights into a number of aspects of ICT and the digital society, roughly 75 years after the introduction of electronic data processing in practice.

Authors from diverse backgrounds, experiences and areas of expertise focus on the information technology, the legal aspects and, for instance, the financial side of digitalisation. In the Netherlands, the initial version of the CoronaMelder app cost €5 million, but Germany spent four times that on the building of the Corona-Warn-App. Some countries opted for technical transparency in this respect, to eliminate citizens' concerns about secret data processing and (mass) surveillance. In the Netherlands, the app was developed publicly from the start — a first for a central government automation project — while the source code of the Spanish RadarCOVID app was not published as open-source software until after societal pressure for this.

Also interesting is the question of the legal status of a COVID-19 app. Is the mobile application a medical device as defined in European law? The collection also devotes attention to ethics and ICT Collaborating authors make the case for a new quality approach for digitalisation, humanity by design, while also reviewing the code of ethics of international federation IFIP.

ICT and data processing have definitively emerged from the confines of IT professionals. The collection Multidisciplinary Aspects of COVID-19 apps has explicitly been written for a multidisciplinary audience, specifically administrators, professionals and politicians, in part in relation to societal, sectoral, technical and legal aspects of digitalisation.

ISBN 978-90-9034977-0
NUR 820