Corona crisis ‘stress test’ has not fundamentally changed the chosen balance between AI innovation and privacy

pwc

June 2020

COVID-19 crisis justifies a new look into scenarios on how artificial intelligence might develop.

As parts of the world start emerging from the aftermath of the COVID-19 crisis, governments have been weighing secure ways of reopening their countries. Despite the differences in approaches, almost every country has been looking at digital solutions as a way to support the safe reopening of their economies.

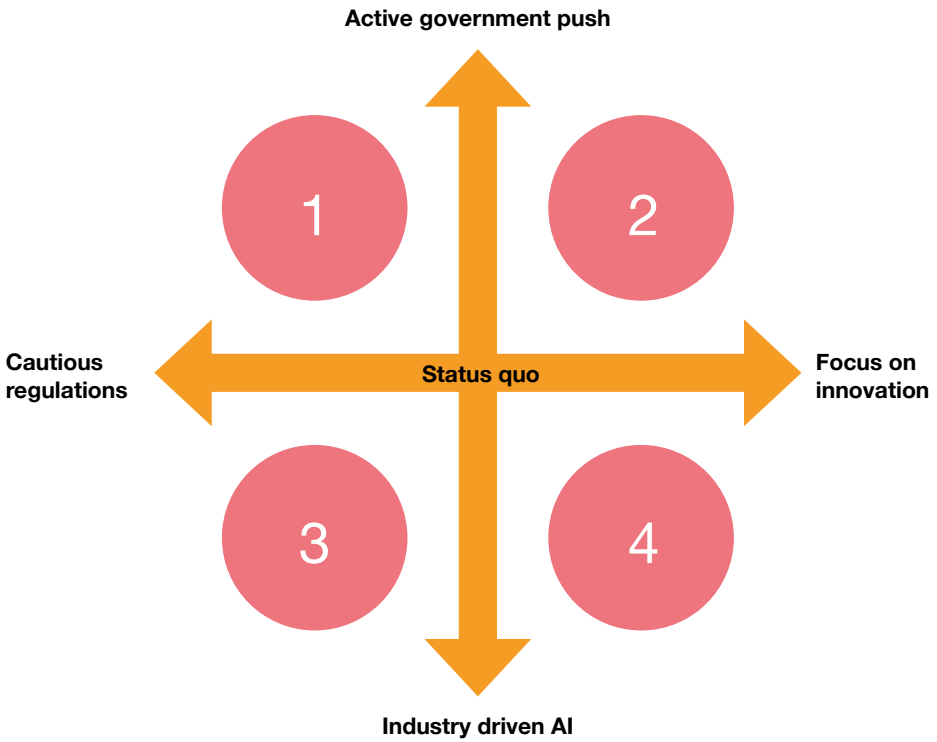
In our report ‘The many futures of Artificial Intelligence’ (see textbox) we looked at the choices and trade-offs governments make, that are decisive for the way artificial intelligence is developing. We developed four scenarios and tested these against the reality of four countries. The COVID-19 crisis justifies a new look into these scenarios and the reality of the projected countries.

We assumed that the deployment of applications that support the containment of the virus (tracking apps) might have changed the balance between innovation and data privacy. We were also curious about the question whether the role of governments as drivers of the development of these solutions might have increased. After the analysis we conclude that at a high level, the approaches did not fundamentally change. Countries that were cautious in their data regulations continued to be wary of quick implementation of tracking apps without fully understanding their implications on privacy. Yet there were some subtle differences in their actions during the crisis, such as an increased role of the government in developing the apps, which are also worth noting.

The many futures of AI

In our report ‘The many futures of AI’, we elaborated four scenarios of what AI may look like in the EU in 2025. These scenarios are based on two questions or uncertainties: will governments actively stimulate and direct the development of AI, or will they leave that to the free market? And do governments apply strict regulations around data collection, algorithms and the market power of large tech companies, or do they prefer a more liberal legislative framework? We tested these scenarios against reality in a number of countries, namely, China, UK, US and the Netherlands.

In the report ‘The many futures of Artificial Intelligence’ we show that the perfect future for AI does not exist. It does show, however, the consequences of government choices and what companies can prepare for. Looking at these scenarios, it becomes clear that trade-offs will be made and that different levels of legislation will have different results for the future of AI. In a scenario where the government is pushing the development of AI (for example, by investing in certain priority areas such as health care) within a strict regulatory framework, the development of AI is slowing down. The “benefit” of such a scenario, however, is that the adoption of AI applications is easier because the confidence of citizens is greater. In a scenario where the development of AI, with minimum government rules and self-regulation, is left to the market, citizens’ confidence in such technology is much lower. However, the advantage is that AI develops much faster, because there is more room to experiment.



Development of tracking apps makes dilemmas surrounding artificial intelligence urgent and concrete

Artificial intelligence has been on a steady path to growth over the past few years. As more and more applications reached technological feasibility, decisions needed to be made on what AI would look like in the future - what applications are acceptable, who controls its development and regulation, and how it will be governed going forward. While data privacy is talked about often as a key concern, the governance of AI is also about taking a wider, more responsible approach towards its development and use. It is as much about data privacy and security as it is about ethics, ensuring fairness and non-discrimination, and explainability of applications. While such concerns are more widely talked about in the context of AI, it has never been more concrete as in the approach towards developing and implementing coronavirus tracking apps.

In the AI report, we hypothesized that the two uncertainties - regulatory environment and extent of government interventions – can give rise to four extreme scenarios which could play out in any country. How cautious are the regulations? Will a country be willing to make some leeway to speed up innovation? How much of an active push will the government be willing to make to develop AI? Each of the four scenarios was already being adopted, atleast in some form, somewhere in the world.

But that was the pre-corona world. In the last months, countries have been faced with the most unprecedented challenges. Governments have been urgently seeking new and innovative tools to help tackle the crisis and save lives. Some countries have been collaborating with telecommunication service providers to access geolocation data to track population movements, enforce quarantine and inform policy decisions. Others have introduced tracking apps to trace and track individuals that have been exposed to the virus, and yet others have been using digital technologies to gather symptom information and disseminate information among the population.

We looked at how the four countries in our original scenarios acted during the crisis. It gives us some insight into how countries might be shifting their priorities in subtle ways. Have their actions around tracking apps, data gathering and other digital solutions been in line with their stand at the beginning of the year? Have priorities evolved, and what could be the impact of the choices being made now?

Choices made since the corona crisis

While there are many ways in which digital technologies are being experimented with to tackle the coronavirus, mobile tracking apps are perhaps the most widely used one. There are various ways in which choices made by governments could be judged – on their impact on data privacy in the short-term, their effectiveness in tackling the pandemic spread and perhaps most importantly, its ability to act as a precedent, demonstrating future choices that governments could make.

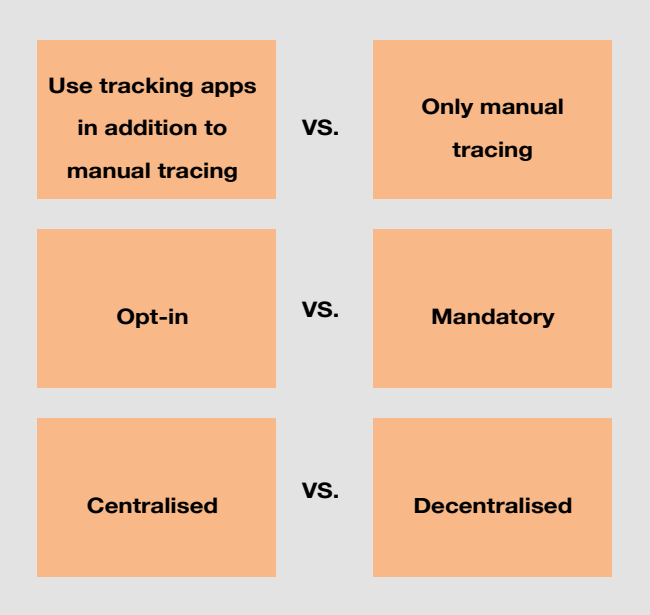
- **Manual or mobile based tracking**

The first among the multiple trade-offs available is of course to use mobile phone based tracking apps. The alternative in use, manual tracing of possible exposures has been widely used by all countries. When it comes to protection of personal data, manual contact tracing – which has been "mandatory" in its use, also has privacy implications, as procedures are not designed to be private and secure.

- **"Opt-in" or mandatory use of apps**

Among other trade-offs available is whether tracking apps are "opt-in" or mandatory to use. The efficacy of opt-in has so far been fairly low because of its low uptake in many countries. At the same time, making its use mandatory when data protection is not ensured, has significant privacy implications.

The many trade-offs



- **Centralized or decentralized models**

Lastly, and perhaps the biggest debate of it all, is the model that the tracing apps use. There are two ways contact tracing apps work – "decentralized", where all relevant contact and location information is held only on users' phones and "centralized", where at least some data is stored centrally allowing for more analysis to be done and more insights gained from it. There are more questions on how these apps work – whether it captures a phone's location, how data is anonymized, if it allows for reidentifying people from anonymized data and for how long (where, and for what) does it store data, if any. Apple and Google have collaborated and promoted a decentralized model, developing a set of interfaces to support a contact tracing app for iPhones and Android phones.

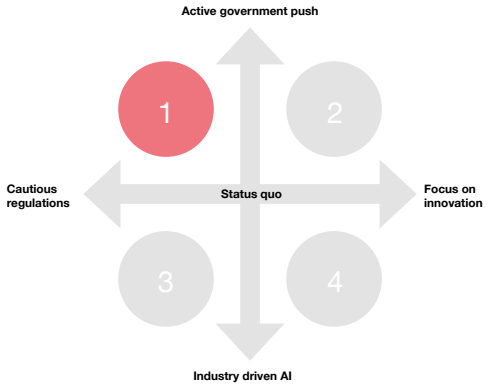
Countries have been evaluating the different models, and making choices based on their expected efficacy and results from initial trials. The UK, Norway, France are among countries that have favored the centralized approach, while Germany, Italy, Switzerland, Austria, among others, have looked towards the decentralized model. There are differences in how each country has approached this complicated issue, yet the choices being made are not only important but also revealing. For example, countries have started with one approach, but after criticisms changed course. Others have been more cautious, and have evaluated multiple apps with details made available to experts and the public. All such actions are indicative of the stand that regulators have on the innovation vs. privacy debate.

Scenario 1: Sustainable AI - preparation meets opportunity Country in focus: United Kingdom

What does the scenario look like?

This scenario has some typical characteristics because of the trade-offs made, such as:

- Slower development of AI due to stricter regulations. Development of AI applications is slower, but the ones that eventually enter the market are promising.
- The government's focus determines which applications are given priority and are stimulated.
- Because consumers have confidence in applications, they adopt them relatively easily.
- Tech companies, including start-ups, compete on the basis of data security and data privacy.



Not all of this apply to the UK specifically, but it is indicative of some of the choices made by the country. The UK has adhered to the same cautious AI regulations that apply to the EU, specifically with respect to data protection. The UK government has consistently been pushing AI development, identifying AI and data as one of four areas in which the UK can lead the world in technology in its Industrial Strategy.

Did the UK make other choices during the crisis?

The UK has largely been following a cautious approach on data regulations. As a part of its corona crisis response, it announced the launch of a mobile phone contact tracing app in April. The app, developed by NHS's technology and research arm NHSX, is currently being tested on the Isle of Wight before becoming nationally available by June. The app uses Bluetooth and keeps records of whom a person meets. Data is stored no longer than 28 days. If a user or contact declares they have symptoms, the app sends notifications to everybody on that list advising them to self-isolate. While there is no requirement to have a test, the government announced that for the trial, anyone who reported their symptoms will be brought a testing kit. The UK has taken a "centralized" approach, in that it plans on storing some data centrally which will be accessible to the NHS to analyze the spread of the pandemic.

Yet, the UK's approach has not been free of criticism. Concerns have been raised, especially the part where some of the data is stored centrally. The data is anonymized, and only uploaded when people declare symptoms, yet there are valid concerns for privacy. While it has been said that some of the data could be used for subsequent "research purposes" related to public health, without complete information on what those uses could be and how data will be protected, potential mission creep remains a concern for users.

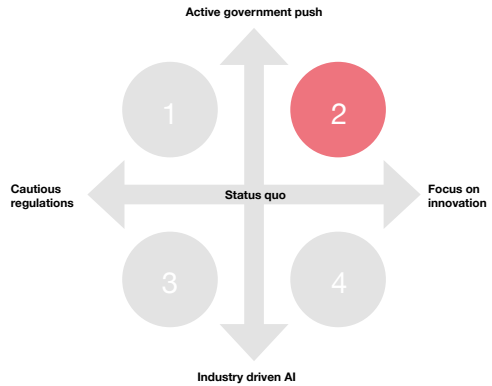
The app has been developed by VMware Pivotal, with NHS, NHSX and the National Cyber Security Centre (NCSC) involved. The active government involvement that we discussed previously has largely remained consistent in the UK's response to the corona crisis, yet how it will use the data collected from its centralised app is still to be seen.

Scenario 2: Growth-oriented AI - the eye on the prize Country in focus: China

What does the scenario look like?

The key characteristics of this scenario include:

- Rapid growth of AI applications by a government pushing innovation and investment.
- Government policy determines which AI applications are given priority and sometimes even which are restricted or prohibited.
- At the same time, large tech companies and smaller start-ups are developing commercial applications on a large scale.
- Consumer confidence is shaky, but both government and business are striving to maintain this confidence.



China has been the classic example of this scenario - with the government being very actively involved in the direction AI development takes, while also focusing heavily on innovation.

Did China make other choices during the crisis?

Since the start of the pandemic, China has been one of the most active users of tracking apps as a means to control the spread of the virus. Once the virus spread began to slow down in the country, local governments began easing restrictions and private companies, in partnership with Chinese government agencies, began rolling out app add-ons to facilitate safe public movement.

The app that has been referred to as Alipay Health Code, has been the most important one in the country. Once a user joins, the app assigns them a color code that indicates their health and access status (like free to move, self-isolation or quarantine). These codes have then been used to allow or deny access to public places, including many offices, parks, restaurants and malls. Currently, people register and generate their codes using Alipay and WeChat, which are ubiquitous apps in China, with multiple applications. While details on how people are exactly classified into the color codes are unclear (except that it is loosely based on travel and medical history), its use has grown since its launch.

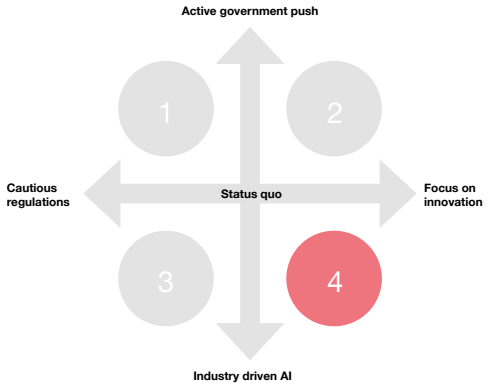
China was relatively quick in developing and implementing the tracking app in the country. The country's focus on innovation first remains consistent with its earlier approach. China also has consistently taken a government-driven approach to new technologies. While many private companies have reportedly been involved in the development of the app itself, its overall strategy as a country is still very singular, largely driven by government agencies.

Scenario 3: Experimental AI - fail faster, succeed sooner Country in focus: US

What does the scenario look like?

This 'extreme' scenario features include:

- Accelerating AI development due to large investments in AI applications by large tech companies, which continue to take over smaller start-ups.
- Investments go in all directions, with many applications being commercially unfeasible.
- Large companies themselves lobby for regulation or self-regulation to maintain consumer confidence.
- Slower adoption of AI applications because consumers in the EU are sensitive to privacy issues.



The US symbolises this scenario, by maintaining a very 'free market' approach to AI development. The country has been more vocal about regulations not hampering innovation potential in the country.

Did the US make other choices during the crisis

There has been a lot of activity in the USA regarding the development of apps for tracking the coronavirus. Notable among them is the decentralized model developed by Google and Apple. There are various other apps developed in the country too, though there isn't a single one that is used centrally by the federal government. Some states, like Alabama, North Dakota and South Carolina are the first states to commit publicly to using Apple and Google's contact tracing technology in their state specific apps.

The prevalence of multiple apps, and a more state-specific approach will enable easier comparison for consumers in the country. This could mean a more choice-driven environment than just an "opt-in or not" decision for consumers, but could also mean lower efficiency of the apps, as inter-state travel complicates tracking by state-specific solutions.

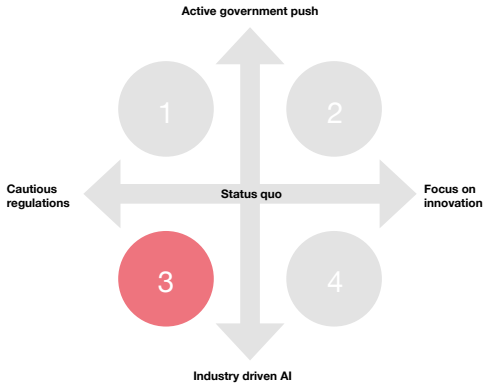
The USA has largely relied on the industry to develop almost independently the apps and related approaches.This fits in perfectly in its long standing approach of letting the industry take the lead on innovation, without a lot of direct government control. On the regulations front as well, the approach remains largely the same. The country is focused on innovation, with the industry setting standards on what it thinks is best for consumer data privacy. While this does not necessarily mean less or weaker regulations, it points more towards self-regulation than the role of central agencies as in many other countries.

Scenario 4: Cautious AI - the balancing act Country in focus: The Netherlands

What does the scenario look like?

The key characteristics of this scenario include:

- Slower development of AI due to legal restrictions on data usage and algorithm control.
- Large tech companies are under pressure because they have to comply with guidelines on privacy and algorithms and therefore have difficulty in recovering their investments.
- Growing concerns about the market power of the big tech companies and pressure on governments to set limits on how they collect and apply data.
- Adoption of AI applications is starting later than expected because consumer confidence is not easy to gain.



The Netherlands has also adhered to the strict data protection regulations that have been characteristic to the EU. At the same time, many Dutch companies have been early adopters of AI and have been moving towards more advanced applications.

Did the Netherlands make other choices during the crisis?

Like other countries, the Netherlands also started exploring the possibility of using digital tracking apps to facilitate the opening of the economy. Earlier in April, the government evaluated 750 proposals for such apps, and held an “appathon” and with seven promising apps, but none of them met the requirements set by the government. Later comments by the government said that there will be no haste in launching the app till security concerns were addressed. Since the country did not accept any of the solutions available yet, it remained unclear if they considered a centralized model at all. While more details are not yet available, the government could develop its own app with experts in the field of information security, privacy, fundamental rights, national security and inclusion.

The Netherlands also used an app as a symptom checker through the Corona Check app (originally developed by a.o. the OLVG Hospital, which was later made accessible to all). It helps doctors diagnose coronavirus in patients – patients can input their symptoms which are checked against RIVM guidelines on coronavirus symptoms. If the symptoms match, a doctor would call the patient and proceed with the diagnostic procedure.

The Dutch government is currently developing a corona dashboard to help further contain the coronavirus. In this context, the government has submitted an emergency law to the House of Representatives that makes it possible to monitor citizens’ mobile phones in order to signal the gathering of large groups of people. The House of Representatives has not yet agreed to this legislative proposal and the law is also raising social arguments.

The Netherlands has remained largely cautious on the corona tracking app. While it recognized the need for an app, and the benefits it could bring, the country did not (yet) accept any solution till all privacy concerns were addressed. On the vertical axis, the extent of government involvement in the Netherlands has been higher than it was in the pre-corona period. We could consider this as a subtle shift from scenario 4 towards scenario 1, where the role of the government is more active than before.

The post-corona world

The post-corona world will undoubtedly be different. The decisions made during the recent past and in the coming few months will have a significant impact on how regulations will shape up for the next few years. While the health emergency will and perhaps should weigh on the decisions made, this is not the only, or even the last emergency that will pose this dilemma between public welfare and privacy. We are careful not to draw any far reaching conclusions yet, since this is a crisis when governments could change courses frequently. Yet it is important to remember that true character is revealed in the choices we make under pressure, and the greater the pressure, the deeper the revelation.

The corona crisis has not fundamentally changed the chosen balance between privacy and innovation

Contacts

Mona de Boer - Data and AI expert, PwC The Netherlands
mona.de.boer@pwc.com
Tel. +31 6 1088 1859

Jan Willem Velthuijsen - Chief economist PwC, PwC The Netherlands
jan.willem.velthuijsen@pwc.com
Tel. +31 88 792 75 58