Global Forum
Shaping the future 2021

In the framework of the upcoming Global Forum 2021, planned for December 6th & 7th in Muscat, Oman, should the pace of this pandemic subside, four preparatory thematic webinars, featuring contributions, reflections and dialogue among key experts and interested stakeholders, are organized.

*This report sums up the discussions of the Global Forum Thematic Webinar II.*

# Global Forum Thematic Webinar II

April 7th, 2021

## TOPIC 1

# COVID-19 Pandemic as a Science and Technology Accelerator?

The Global Forum Thematic Webinar II on "COVID-19 Pandemic as a Science and Technology Accelerator & Disruptive Digital Technologies, Artificial Intelligence, IoT, 5G, and Blockchain" took place on April 7th, 2021 from 13:30 to 15:00 UTC+2 via Zoom.

**About 60 participants joining from all over the world—for some it was very early in the morning, for others late at night—made this webinar a particularly intense and thought-provoking one. Framed by brief expert presentations, the participants engaged in high-level debates and deep discussions on critical issues and opportunities.**

It was the second of a series of four live webinars (the next will be on June 9th, 2021) featuring contributions, reflections and dialogue devised for the purpose of feeding the framework of the upcoming Global Forum 2021.

## AGENDA

### Topic 1: COVID-19 Pandemic as a Science and Technology Accelerator?

**Stéphane Grumbach**, Research Director, INRIA, France
Living under a long-lasting Pandemic & Impact on the Evolution of Technologies

**Amir Johri**, Senior Specialist, Ministry of Health of Oman
The Role of Digital Enablers in Coping with the Pandemic – Examples from Oman

**Paul Wormeli**, Innovation Strategist, USA
Cross-boundary Information Sharing Principles – Complexities and Challenges

---

**Stéphane Grumbach, Research Director, INRIA, France, opened the discussion with remarks about living under a long-lasting pandemic and the impact on the evolution of technologies.**

It is better to be resilient and try to adapt to whatever might come, rather than just trying to go back to how the world was before.

The Covid-19 crisis has fundamentally affected our societies: The limitation of liberties, such as movement restrictions or the type of meetings people are allowed to have, rise central questions and are politically very controversial. Many sectors are suffering, and some might collapse. Societies are facing new logistic challenges and there is a much stronger uncertainty in making plans. Covid-19 led to the emergence of new behavioural norms (the way we greet each other, the way we organise meetings etc.) and new forms of organisations. The pandemic also reshuffles things on the political and geopolitical spectrum.

It is a point in time where many aspects of our lives are reshaped—with a huge potential for both good and bad, and it will be important to reflect on what can be done and what should be done. Technologies play a central role. They fundamentally contribute to keep parts of our societies functioning and determine basic dimensions of our society, such as the way we meet and move, how people can exchange, but also information processing and data access. One particular aspect is the use of technologies in the fight against the virus.

Still, even before the pandemic, digital intermediation platforms already changed the way we exchange (e.g., emerging commercial and educational platforms, home delivery etc). These platforms have been essential to keeping societies functioning during the pandemic.

There are various ways to fight COVID-19 using IT, such as contact tracing, real time mapping of the spread of the disease, population monitoring or the use of coercive measures. The majority relies on smartphones linked to private actors, such as the large intermediaries, and public actors, i.e., health authorities, research institutes, police etc. These approaches are rather controversial and reveal strong geopolitical tendencies.

The way companies like Apple, Microsoft, Amazon, Alphabet, Facebook, Tencent or Alibaba increased in market values during 2020 is impressing and demonstrates the increasing universal control of platforms.

The technologies used to keep our societies functioning are mostly technologies that emerged in the last 20 years, provided by companies that are becoming the most powerful actors from many points of view. The large digital platforms are the largest market caps today and conflicts between these digital platforms and territories are multiplying. Besides, those platforms compete with national public administrations with regards to the services they provide.

We should take the opportunity of the current crisis to rethink services and service provision. For instance, the tools that are currently used for education are fine, but they are not good enough to provide effective distance learning. The same applies for health and many other sectors. Another issue is the use of IT tools to fight the virus. These surveillance tools are extremely controversial and raise privacy and civil liberties concerns, especially when there is no real trust in the state. How can one be sure that the harvested data are used only temporarily and exclusively to fight the spread of the virus?

There is a real opportunity to rethink essential services that would make societies more resilient in times of crisis and we should take that opportunity.

**Comment/ Question 1:** Referring to the issues of dissatisfaction with remote learning and trust in governments, it was argued that some Scandinavian countries have done rather well, and those are the countries where the state is generally trusted. The question seems to be less about how the technology is used, or the competence of the governments or the big companies that are using it, but more about political culture and the pre-existing trust, the way things are presented, i.e., the people are being given clear and straight advice.

**Stéphane Grumbach** replied that at the beginning, European countries started developing contact tracing applications and most of them ended up proposing the Apple/Google solution. People finally had greater trust in Apple and Google than in their governments.

Singapore just passed a bill governing police use of contact tracing data to collect evidence. Imagine there is a crime, and you have the contact tracing application in use, which means that you can see who has been on the crime scene. Will you use it or not? And if you use it for a crime scene, you might also use it for something else… This question of trust is much more general and applies to everywhere in the world.

With regards to the general dissatisfaction with remote education during the pandemic, it has to be said that education has to be fully reinvented—regardless of the crisis. Currently, we just reproduce in the digital space what we do in the physical space. But the digital space allows things that are completely different, and we don't really use that. We should take this opportunity to promote other ways of organizing education, health etc.

**Comment/ Question 2:** Due to climate change, wildfires, disappearance of many animal species, there will be more and more frequent sanitary crises in the future. However, the acceleration of change that has been witnessed in 2020 gives room for optimism. We could be capable of being more resilient, predictive, and ready to face such crises.

**Comment/ Question 3:** GSMA has just completed a project as part of its AI for Impact work - with foreign aid funding from the UK and in partnership with mobile operators and national governments - using big data analytics to address specific challenges of the Covid crisis across 14 countries. The report will be made available on the Global Forum's website.

**Comment/ Question 4:** The pandemic has accelerated the adoption of digital technologies. The broad adoption of remote processes, smart systems, and advances in virtual and augmented reality, led to a rise of what some people call "tele-everything".

---

**Dr. Amir Johri, Senior Specialist, Ministry of Health of Oman, presented examples demonstrating the role of digital enablers in coping with the pandemic in Oman.**

Digital technologies are being used in a very practical way by the Ministry of Health in Oman.

The Ministry of Health's *Tarassud* mobile app provides residents of the Sultanate of Oman, with transparent information on the spread of Covid-19, e.g., the number of cases and how the cases are increasing, the infection rates in the different parts of the country, but also information related to the vaccination campaign.

Moreover, the application informs about SOPs issued by different organizations and the Ministry of Health for both the general public and the Ministry of Health employees. It also updates on ministerial decrees, new laws and new information coming day-by-day.

Another application developed by the Ministry of Health in the effort to limit the spread of Covid-19 in Oman is *HMushrif*. Its objective is to ensure compliance of people who are being quarantined (both in institutional quarantine and home-based isolation) with the quarantine rules. A digital wristband is given to individuals put under quarantine to trace whether they are maintaining the quarantine or not.

*Tarassud +* is a powerful technological solution and extremely convenient. The application can be used while being in another country: people just download the app, they pay online, they know where their Covid-19 test can be done and they receive the results on the app, which then can be scanned at the airport.

These applications go hand in hand and digital technology was a great help in fighting the pandemic in Oman with regards to information, data collection, and analytics. It has been used responsibly, and the Ministry of Health is looking forward to a more widely use within the general population.

**Comment/ Question 1:** Stressed that people are aware of the change that happens in Oman. There is an increasing general acceptance of using digital tools. People don't really feel traced by the applications, but rather informed about Covid-19 and the spread of the virus, which has helped to keep the virus under control.

**Comment/ Question 2:** Added that young people in Oman used additive technologies, like 3D printing, to produce mundane consumables, such as face shields etc. One group even produced a breathing machine. And regardless any market success, this group of youngsters

innovated—or at least used technologies and localised the manufacturing to catch up with the crisis. Other young people developed applications to meet the changing societal needs.

It seems to be an opportune time to help local entrepreneurs localise manufacturing—not necessarily in the digital domain—but of very mundane consumables. Once you do this, innovation follows. For instance, there are a lot of people who can make masks. Start with this and then go further: Why not producing a mask that indicates when it is contaminated? One could use a specific patch indicating whether it is contaminated or not. You do not even need electronic sensors.

---

**Paul Wormeli, Innovation Strategist, USA, addressed the issue of cross-boundary information sharing principles, emphasizing that a discussion on the impact of the pandemic couldn't be more timely.**

Last week, on March 30, the Science Academies of the G7 countries issued the statement: "The nations of the G-7 and beyond should work together to adopt principle-based governance systems for securing safe sharing and use of data for health emergencies; build and implement the operational systems, infrastructures, and technologies for implementing a principle-based and privacy preserving approach to equitable use of data for health emergencies".

It is a striking call that puts us all in the picture of deciding how technology can really be valuable for dealing with future pandemics. Over the last decades, we have established some fundamental truths about this. The problem of doing what the G7 Science Academies has suggested, is that we must understand some of these truths very carefully. We know that collaboration is the only way to make substantial improvements in the quality of government services. We also know that information sharing is essential to enable collaboration, but we don't do that very well on a global scale. Moreover, experience has shown that cultural impediments outweigh the technical issues in figuring out how we can share information with each other, and that the complexities increase exponentially as the scope of sharing increases.

To establish trust in governments, we have to balance the privacy policies and build the trust in the communities that support governments. And we must figure out how to balance privacy policies with interoperability and global data standards. And all this must be built on a system of governance—which we are not very good at on an international scale, especially in areas like information sharing.

It's a real challenge, but we are not starting from scratch: Back to the 1950s, the OECD created the "Fair Information Practices". These fundamental principles are at the heart of the U.S. Privacy Act of 1974, the EU General Data Protection Regulation and other laws, but they haven't been revisited and refined since. Nevertheless, some of these principals are still very important to the population, especially the principle of ensuring that data is used only for the purposes for which it was initially authorized.

These practices that were developed on an international basis need to be revisited and re-examined in today's world of technology. And we can go beyond that: We have the opportunity to develop principles of safeguarding data. Technology must be a means for

protecting privacy and securing information, and we must find innovative and new ways to use technology to support the protection of individual privacy. In this context, standards are essential for supporting sharing innovation and safeguarding assets. People are more and more considering information as an asset that must be safeguarded. We have to come up with more international technology independent agreements governing privacy. One of the key difficulties, as well as opportunities, is that we need to have more effective safeguarding technologies that deal with the issues of federated identity and privilege management on a global scale. This is no simple matter, but there are already technologies that are very exiting in terms of how this could be done on a global scale.

What we need is the political consensus and the establishment of an international global will to deal with this—or, as Ronald Reagan put it in 1987: "Tear down this wall! "

**Comment/ Question 1:** Wondered how the actual geopolitical setting, which is very conflictual with regards to cybersecurity, will impede or help accelerate international agreements.

**Paul Wormeli** explained that we must start with the policies that we would like to implement and then let the technologies enforce those policies. Cybersecurity is a very particular discipline that can be used to bring people together. In the U.S., the new Cyber Domain and the National Information Exchange Model are building standards on how to report and manage cyber incidents and come up with real time responses to cyber-attacks.

Cybercrime is an international phenomenon that must be dealt with on a global level. We have to figure out what we want to have accomplished and what the objectives are and then assign this to the technology.

**Comment/ Question 2:** Pointed to the fact that different countries have different perspectives and objectives. It might be difficult to reach consensus.

**Paul Wormeli** replied that the OECD demonstrated that it is possible. The UN Commission on Crime Prevention and Criminal Justice also has built an International Classification of Crime for Statistical Purposes and 170 countries have agreed to work together. It is possible, if we find the right format and organizational framework for doing so, but it requires good will and dialogue—it can't be done in a vacuum. It must be consensus based, not based on regulation.

**Comment/ Question 3:** Added that we might need both, good will/consensus and good regulation that supports individual privacy but also tries to underpin those common rules.

**Paul Wormeli** agreed by stressing that the way to get there is the building of consensus. Regulation without involving the stakeholders tends to be nothing more than conflict.

**Comment/ Question 4:** Referring to the development of broad-based international consensus around governance questions, it was added that such common principals reflect values. The challenge is that there is internationally a great disparity as to values that underpin governance questions. In terms of moving to common principles, it might be a good starting point to begin with the likeminded parties, which are essentially democratic oriented societies and do have an underlined sense of values in this area. Maybe a broader consensus then goes beyond what is possible, because, a heart, technology competition is a competition of values.

**Comment/ Question 5:** We need clear and strong principles for information sharing, especially regarding security and privacy. One first issue is the difference of vocabularies and semantics that exist among world nations, e.g., in the U.S. and EU there are slightly different meanings for “privacy”. We need to set up a dialogue (the OECD could be a starting point, but we need to look beyond). Second, cooperation makes sense if it takes place over time, i.e., several years, not only when the principle meets temporary political interests.

**Comment/ Question 6:** The OECD is less than 20% of the world population and most of the largest countries, incl. the big actors in IT, are not part of it.

**Comment/ Question 7:** The OECD could be a starting point because of its potential reactiveness. But indeed, the dialogue must be spread over as many countries as possible, even if as we collectively suffer from a lack of common understanding on concepts, values, principles etc.