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, three 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 I.

Global Forum Thematic Webinar I

March 3rd, 2021

Wireless & Wireline Infrastructures: The Upcoming Challenges

Designing a Regulatory, Policy, Governance Framework Addressing Safety, Security & Accountability in a Complex World

Participants (64):

Ahood Said, Sylvie Albert, Wafa Almamri, Pras Anand, Ingrid Andersson, Sherif Aziz, François Belorgey, Youssef Berbash, Jean-Pierre Bienaimé, Katherine Blizinsky, Marek Canecky, Jean-Pierre Chamoux, Delphine Chevallier, Mariane Cimino, Donald Davidson, Bob Deller, Koffi Fabrice Djossou, Isabelle de Michelis, Kevin Fitzgibbons,John Giusti, Stéphane Grumbach, Alessandro Guarino, Nitya Karmakar, Hugo Kerschot, Latif Ladid, André Laperriere, Corine Le Mouel, Sébastien Lévy, Andy Lipman, Judith Logan,Tom Mackenzie, Samia Melhem, Eunika Mercier-Laurent, Jeremy Millard, Michele Mosca, Sylvain Nachef, Eikazu Niwano, Alice Pézard, Pascal Poitevin, Hervé Rannou, Joël Ruet, Gérald Santucci, Patrick Saunier, Gary Shapiro, Alan Shark, Dan Shefet, Dan Shoemaker, Tamara Shoemaker, Susanne Siebald, Jean-François Soupizet, Baïla Sow, Lara Srivastava, Michael Stankosky, Bénédicte Suzan, Yoshio Tanaka, Sylviane Toporkoff, Daniele Tumietto, Eliane Ubalijoro, Rob van Kranenburg, Daniel Van Lerberghe, Oliver Väartnou, Olin Wethington, Paul Wormeli, Sarah Zhao.

The Global Forum Thematic Webinar Ion “Challenges of Wireless and Wireline Infrastructures and Regulatory, Policy, Governance Frameworks in a Complex World” took place on March 3rd, 2021 from 13:30 to 15:00 UTC+1 via Zoom.

With more than 60 participants joining from Asia, Europe and Africa, and the USA and Canada, it was a well-attended, particularly dynamic and highly interactive webinar with intense Q&A sections and lively discussions.

It was the first of a series of three live webinars (the next will be on April 7th, 2021) featuring contributions, reflections and dialogue devised for the purpose of feeding the framework of the upcoming Global Forum 2021.

Agenda

Welcome and Introduction

Topic 1: Wireless & Wireline Infrastructures: The Upcoming Challenges

John Giusti, Chief Regulatory Officer, GSMA

Food for Thought Questions:

- How important is 5G for the digitalisation of the economy?
- What is the role of government in extending broadband access to everyone?
- How do you see wireless and wireline infrastructures being used to support climate action?
- How should governments incorporate network connectivity into its recovery plans and economic stimulus packages?

Latif Ladid, President, IPv6 FORUM

- IPv6-based New Internet empowering Super IoT, Standalone 5G, Data Sovereign Cloud Computing

Q&A

Topic 2: Designing a Regulatory, Policy, Governance Framework Addressing Safety, Security & Accountability in a Complex World

Andrew D. Lipman, Partner and Head of Telecom Group, Morgan, Lewis & Bockius, USA

Food for Thought Questions:

- How, if at all, has the corona virus affected telecom and tech laws? How should have it impacted existing laws, where such changes have not yet occurred?
- Are these changes temporary during the pandemic or permanent? Should they be permanent? Should the laws treat high speed broadband as a Human Right?
- Will we continue to see more deregulation of the Telecom and Tech center or is there the need for more regulation, not less, to serve societal goals?
- Are US and EU Telecom and Tech laws becoming increasingly biased against the Chinese? Are we risking a bifurcation of tech systems between the West and the East? How can these laws be changed to be more open to Chinese vendors?
- Should telecom and tech laws be strengthened to protect consumers from privacy violations by the Social media companies.
- How can Telecom and Tech regulation and laws ensure the benefits of technology are more equally distributed to low income and other historically disenfranchised groups? Where have existing laws failed to achieve this objective?
- How can Telecom and Tech laws and regulations better address issues of social justice and racial equality? Where have existing laws failed to achieve this objective?

Jean-François Soupizet, Senior Advisor & Independent Expert, Paris, France

- Recent trends in the regulatory spere in Europe and its future implications

Q&A

Concluding Remarks

Welcome and Introduction

The webinar's moderator, Ingrid Andersson, together with Sylviane Toporkoff, welcomed the participants and provided a brief introduction to the upcoming 90 minutes.

Focussing on two main topics around virtual infrastructures and regulation, the webinar was the first of a series of three live webinars organized as warm-ups for the Global Forum 2021, planned to take place on December, 6th& 7th, 2021 in Muscat, Oman. (Note: If the pandemic still imposes travel restrictions at the end of this year, the Global Forum 2021will be postponed to March 2022).

Topic 1: Wireless & Wireline Infrastructures: The Upcoming Challenges

John Giusti, Chief Regulatory Officer, GSMA, **opened the discussion on upcoming challenges related to infrastructure by providing a mobile operators' perspective** on these questions.

The GSMA is the global trade association of the mobile operators and represents over 750 mobile operators globally.

According to GSMA statistics,49% of the world's population are connected to mobile broadband. Thus, one half of the world population is not using mobile broadband connectivity at all. Less than 10% of the population lives outside of mobile broadband coverage. The biggest issues are not infrastructure, infrastructure investment or coverage, but barriers to usage, such as digital literacy, relevant content in local languages or affordability. Of course, one needs to address the 9% not covered at all, but a lot of progress can be made if we can find ways to get more citizens to participate fully—those who actually could access, but don't for various reasons.

Never has there been a time where digital economy has been so at the front. The COVID pandemic made that parties engage in discussions like never before. We see the power and the potential of a digital enabled world; the worldwide economy continues to operate under COVID restrictions thanks to connectivity and digital solutions. Online platforms and all sorts of mobile devices have helped citizens communicate, connect and consume more than ever. Healthcare and education in particular have pivoted to digital alternatives. And with 5G network deployment progressing, new connected services and the digital transformation of industry are starting to move forward.

As a result, we are seeing a renewed appreciation of digital connectivity, greater government attention, greater policy maker attention and greater industry attention, as well as an increasing understanding of social and economic resilience through connectivity worldwide.

GSMA considers three key areas of opportunities: 1) the area of 5G rollout; 2) how industry can support climate action; and 3) the importance of considering digital infrastructure in post-COVID stimulus packages.

Regarding 5G connectivity, North America is leading in terms of 5G adoption in percentage to its population, whereas the Asia Pacific is leading in overall numbers. According to GSMA 5G deployment projections, China will continue to dominate global 5G connections. With 5G already available across Asia and North America, the majority of new launches continue to be in Europe. Global 5G connections are projected to reach 1.8billion, by 2025.North America, Europe and Asia Pacific will account for 90% of 5G mobile connections forecast globally by 2025.

However, a number of countries are just beginning their 5G journey and it is time to reassess the investment environment to ensure the ability to invest in infrastructure, whether it be incentives for investment or removing regulatory impediments.

The mobile industry continues to experience declining margins, mostly due to the nature of the markets and regulation. Economic recovery post-COVID measures should support an environment where investment can be facilitated, particularly for those countries facing impediments to keeping up in terms of speed of deployment. Releasing sufficient spectrum, reducing sector specific taxation and streamlining rules around network deployment could free up investment in digital infrastructure and lead to new kinds of solutions and services.

Climate change has become a defining issue. Net global emissions have to be cut in half by 2030, before reaching net-zero emissions by 2050.To achieve that goal, the green agenda of the mobile industry relies on the following three pillars:

First, maintaining industry momentum towards net-zero emissions by 2050. The mobile industry has been very focused on monitoring and mitigating their greenhouse gas emissions. Two years ago, GSMA members committed to reach net-zero emissions by 2050 at the latest. So far, there are 60 mobile operators (representing 70% of all mobile connections) disclosing their climate impacts to the Carbon Disclosure Project.21 of those operators (representing 25% of global connections) are on a path to achieve net-zero emissions by 2050 or earlier using Science Based Targets.

Second, the widespread use of smart and connected technologies across all economic sectors. In fact, mobile connectivity already enables a reduction in the emissions of other sectors (about 10 times of the mobile industry’s own carbon footprint). This is referred to as the ‘enablement effect’—an effect that could double (to 20 times) by 2025, due to the increased prevalence of other connected technologies.

And third, mobile enabled solutions for climate change resilience, i.e., helping low- and middle-income societies adapt. This part of the green agenda implies collaboration (particularly with emerging economies) on how digital technologies can help respond and support the transition to a low carbon economy but also to a climate change resistant one.

The third area of key opportunities to be mentioned are national economic stimulus packages and post-COVID recovery plans. Governments all over the world are devising ways to rebound from the economic crisis caused by the pandemic. The 750-billion-euro recovery fund of the EU, for instance, aims at strengthening the single market but also at adapting to the digital age, including investing in more and better connectivity, as well as building stronger industrial presence in AI, security, supercomputing and cloud. Such focus on a digital and green recovery seems to be the right path, while at the same time considering connectivity.

Samia Melhem commented [via chat]: During the pandemic governments have partnered with telecoms providers to subsidize access and data plans for teachers and civil servants. The pandemic has accelerated the reskilling of teachers (and parents). The challenge is to keep investing in broadband (incl. 5G) and not to neglect digital infrastructure as governments face economic problems and hardship due to declining GDP in 2021.

André Laperriere commented [via chat]: Experience in some regions indicated that a binary definition of access to 3G or 4G led to sometimes misleading conclusions as the poor quality of the connections made a significant proportion of the 'available' connections in reality unusable. What about the access quality of 5G?

Daniel Van Lerberghe asked for more details about the effort to reduce the digital industry's carbon emission and what to answer the strong opposition to 5G?

John Giusti clarified that the transition to net-zero is a pathway, which needs to be specific to each industry. The pathway of the mobile industry will be different from the one of the automotive or broadcast industry. The mobile industry worked with international standards bodies and the ITU on the green pathway to take, starting with climate disclosure. Most mobile connections globally today are provided by operators that are disclosing.

The next challenge is to get the Science Based Targets agreed, which helps to have a very concrete path to get there. Currently, about 25% of the global emissions are covered by the path. The COP26 in November will be an occasion to encourage the industry to do more. For instance, MTN, a South African mobile telecommunications company, just announced two weeks ago their roadmap to get to net-zero by 2040.

The mobile industry has a lot of input from other industries, such as energy and equipment suppliers, that affects the industry's ability to meet the net-zero objective. One big focus of this year is to make sure that these industries are on track.

There are significant 5G deployments, i.e., more than 130 live network deployments globally (Europe, Asia Pacific, North America and the Gulf). The issues people have around 5G and health, are the same issues we had before with 3G and 4G. This issue of electromagnetic field radiation is something that has always been there. There are however problems with social media platforms in the context of conspiracy theories around EMF and health.

The key for the mobile industry is to make sure working with scientific experts to ensure compliance with the international standards. The current 5G deployments are fully compliant, the EMF exposure is even significantly less than people get from other sources.

As mobile networks and 5G are moving to new bands, we need to verify that everything in those bands is within the appropriate safe levels. GSMA We are countering conspiracy theories by communicating as much scientific information from the international community and from independent academics as possible. The issues are really no different than they were with the previous generations of mobile.

Donald Davidson shared [via chat]: link to the NSTAC Report to the President on Advancing Resiliency and Fostering Innovation in the ICT Ecosystem https://www.cisa.gov/sites/default/files/publications/nstac_letter_to_the_president_on_advancing_resiliency_and_fostering_innovation_in_the_ict_ecosystem_2.pdf

Bob Deller asked whether the 5G range of the spectrum is different from the traditional 3G and 4G range. If so, the applications would be different. Are we missing opportunities for enhancements at the 4G and 3G levels by focusing uniquely on 5G?

John Giusti explained that we need to separate the technology from the spectrum band. Some of these technologies are working in some of the same bands. A lot of initial 5G deployments have been in traditional mobile bands, i.e., mid and lower frequencies. The spectrum has the same characteristics, it is the technology that gives increased speed, reduced latency etc.

What is new is the question of some of the higher frequency bands. Those frequencies behave differently and this is where a lot of research is going on. Even if the amount of exposure from mobile is so below the kind of exposure we get from other things in daily life, it is important to ensure sound examination of higher frequency bands. At the same time, it is a bit like a chicken or egg: you can’t do much real-life testing until you have real-life deployments.

5G is a natural evolution of the other technologies and can be deployed in some of the same bands, but some 5G applications are also looking for higher frequency bands. This doesn’t provide higher coverage—it is really about ultra-high speed and low latency in a very contained area. For those applications it is not possible to use the digital dividend spectrum used for broadcasting (which is about coverage, not about high throughput speed).

Bob Deller proposed to invite an expert to the Global Forum addressing these issues.

John Giusti would be happy to share some material on this put together by GSMA.

Michele Mosca underlined the great importance of infrastructure resilience to protect against threats. As we deploy these enabling technologies, we also create a great dependency and great vulnerability. A massive systemic disruption in these infrastructures can be catastrophic for societies all around the world.

Cyberattacks can be very targeted and sustained. Reliance is not something you do once. It needs to be persistently in our minds—just as our health that we consistently maintain and revaluate.

John Giusti agreed. This is a serious danger (which also concerns other forms of critical infrastructures, e.g., power supply).

Network operators are very engaged with cybersecurity, because they have a strong interest in protecting their infrastructure. Experience has shown that they spend a lot of time on cybersecurity, but they don’t talk about it so much. During the early days of the pandemic, there were a number of very targeted cyberattacks attacking hospital facilities and for the most part, the networks were able to manage those attacks. As technology moves very quickly, you need the experts within the industries to have very robust defences. A greater involvement of governments and policy makers in cybersecurity can be noticed.

Vulnerable entry points create an additional risk and are a bit harder to manage. There are plenty of new digital technologies that are being deployed from all sorts of companies that haven’t been involved in digital before.

Michele Mosca commented [via chat]: There is a subtle distinction between security (focused on today's attacks, the risks are largely internalized and appreciated) and resilience (focused on emerging threats and unknowns, where the risks are much harder to internalize and plan for, although it can be next-to-impossible to make up lost time as the threats are realized). It's hard for IT vendors to prioritize resilience if their customers are not valuing it. It's hard for political leaders to prioritize resilience if their voters don't value it. It's a serious challenge.

Some sort of regulation is perhaps the only practical way to internalize the costs of not being resilient and the rewards of (cyber) resilience, and incentive resilience-by-design.

Lara Srivastava commented [via chat]: Therein lies the difference between 'band-aid solutions' and serious proactive/preventive measures. The same goes for data protection: the difference between legislating after the fact, or penalizing after the breach, and creating a resilient and safe human-centric data ecosystem.

Donald Davidson commented [via chat]: This is not just an information systems / network problem—think of IoT connectivity at 5G speeds.

https://www.sae.org/works/committeeHome.do?comtID=TEAG32

SAE G-32 shall utilize and coordinate the knowledge, experience, and skills of technical experts in the field of Cyber Physical Systems Security (CPSS) to:

1. Characterize and address the risk to CPSS, assess vulnerabilities, and recommend System Engineering focused mitigation actions.
2. Share the knowledge of how vulnerabilities are introduced and exploited in cyber physical systems.
3. Document best practices for addressing areas of concern utilizing existing processes, procedures, and standards.
4. Develop a taxonomy for CPSS.
5. Establish standard methods for identifying vulnerabilities in cyber physical systems introduced at any point in the CPSS life cycle and mitigating impacts.
6. Develop validation and verification methods to ensure requirements are addressed.

Jeremy Millard raised the fact that even the World Economic Forum considers deglobalization as current trend. A less globalized world has immense implications for infrastructure and interconnectivity. At the same time, China has made its own Internet and Russia is doing the same. Are we losing the globalised Internet? And what are the implications for infrastructure?

John Giusti answered that one of the big challenges to increase connectivity and inclusion is making locally relevant content more available so that it does become relevant locally and is targeted to local community.

From an infrastructure point of view, the big barrier to deployment is cost, and a fragmented infrastructure (lack of interoperability, bespoke national or regional systems) is going to drive up the cost. It will make it more expensive and fewer people can enjoy the benefits. From an infrastructure standpoint, we have to prioritise global interoperability, standardization and harmonisation wherever possible. There are real risks in this aera—people aren't focussing on the long-term implications, especially for the underserved, if you increase the cost.

Latif Ladid, President, IPv6 FORUM, then continued with discussing **the IPv6-based new Internet empowering super IoT, standalone 5G, and data sovereign cloud computing**.

We are in the third generation of the Internet. The first one was ARPANET, a research network enabling email. In 1981 the Internet (IPv4) came up, which use was then stopped by the US Government in 1985. The Internet finally took on a more familiar form in 1991.

However, as it uses 32-bit addresses, IPv4 provides a very limited number of Internet addresses (about 4.3 billion) and this address space is completely exhausted since 2011.

The work on IPv6 started in 1995, to ensure that the Internet will continue to function properly. IPv6 uses 128-bit addresses to avoid address shortage and provides a number of new capabilities essential for the deployment of new technologies.

IPv6 restores the end-to-end model, which is fundamental for the many of the applications that we are moving to. IPv6 allows to connect all sorts of things, i.e., billions of devices connected to the Internet, and thus empowers the IoT and 5G.

We are currently not using the full potential of the IoT, because the majority of IoT devices connected to the Internet are going through a certain gateway. IPv6, on the other hand, enables peer-to-peer communication. Things talking to things—this is where the real (r)evolution will happen. Instead of people managing the things, things will manage themselves. This is where a global IoT will happen.

There is a real issue when it comes to cloud computing: The cloud computing as it is used by Amazon was developed by a team in Cape Town, South Africa. The fact that Amazon has an AWS (Amazon Web Services) proprietary stack might compromise data sovereignty. Due to Patriot Act and the Cloud Act, NEC has access to cloud computing data around the world, through Amazon based in the U.S.

As a counterweight to the U.S. cloud computing providers, a number of companies from France and Germany initiated the EU cloud initiative GAIA-X. GAIA-X is meant to bring in new standards and follow strict data protection laws. It will not be undermined by "back doors”, which is a fundamental step towards data sovereignty.

In terms of wireless, attention was given rather to some surprise deployments than to the evolution of the mobile network itself: 2G for SMS, 3G for the Web, and 4G for Youtube. Most probably, the same thing is going to happen with 5G and 6G and it will be more the verticals we are going to talk about.

The spectrum used for 4G is below 6 MHz. With 6G we will move to Terahertz frequencies, which are generally considered as innocuous (further testing might be necessary). The THz range has certain limitations: The propagation of THz signals is limited to 10m, they cannot penetrate doors or windows and fail when it rains. Thus, these frequencies are more for indoor usage. For instance, it would be possible to replace the indoor fibre cables in data centers by THz routers.

Currently 2 billion people worldwide are using IPv6 without knowing it.

Topic 2: Designing a Regulatory, Policy, Governance Framework Addressing Safety, Security & Accountability in a Complex World

Andrew D. Lipman, Partner and Head of Telecom Group, Morgan, Lewis & Bockius, USA, **discussed the issue whether we are heading to decoupling the Internet and telecom.**

We need seamless, uninterrupted global telecommunication. The Telecom and Internet industry is the classic economic example of the networking effect: the more people interconnected, the more viable the entity becomes for its owners and users—a principle that is not only applicable on telecom, but also on social media, with companies like Google, Facebook, TikTok, WeChat or Alibaba. Some would say, the networking effect worked too well, in terms of setting up a situation where the "winner takes all". Other would say, however, they rather thrive on global connectivity.

These global networks also create many secondary benefits in terms of technology development, R&D, wireless connectivity, public networks for education or healthcare etc. Because these networks have public utility type and resource scarcity aspects, they have historically been regulated on many different levels. Many of these types of regulation are national security, and, perhaps except nuclear power plants, no other industry is more regulated than telecom.

Over the years, the telecom/Internet industry has learned to overcome and master those growing body of laws and regulations, including dealing with national security issues. Indeed, national security issues have influenced the telecom industry for a century: In 1921, the U.S. enacted the Submarine Cable Act to prevent espionage and sabotage following the lead of the UK and France.

What is new, is that these historical and well understood national security considerations are being arbitrarily stretched to address a lot more than national security per se, but often to be a screen to address unrelated issues, such as economic leverage, domestic politics, trade considerations, or nationalism. Many of these concerns morphed from argumentatively legitimate concerns into irrational, politically divisive and political wedge issues.

Recently, we have seen this in the U.S., the UK and other allied countries against China, Russia and other Asian countries perceived to be friendly to China. China and Russia inevitably retaliated with the Chinese 2025 plan.

These practices, if they could accelerate, could lead to a global decoupling and bifurcation of the telecom and Internet. This decoupling could result in two separate Internets, two separate tax systems… and maybe even more than two.

Over the last two years we have seen a global schism and decoupling of telecom. We have seen the U.S., Australia, New-Zealand, the EU blocking Huawei and ZTE equipment in their networks, and the U.S. blocking Hengtong equipment in submarine cables. The U.S. also revoke the licenses of Chinese carriers; we have seen the submarine cable between U.S. and Hong-Kong be blocked; and most recently restrictions on social media (Alibaba, TikTok, WeChat). The practices are going on and are spreading to others countries—and in reverse in China and Russia. The result would be a calamity of insular bifurcated decoupled networks.

National security is crucial and very important for Internet and telecom, but we should focus on the pure national security concerns and not get mixed up and diverted by other pretexts for economic and politics issues. While there is inevitable tension between open communication and natural security, we need to find smarter ways.

To conclude, we should

1. break this increasingly dangerous circle. All governments should recognize the importance of telecom and tech connectivity and resort to minimum affecting national security remedies where possible.
2. dial back the overreaction leading to decoupling. Make sure to address truly legitimate national concerns and don't get diverted by economic nationals and the big power politics.
3. recognize that open robust telecom facilities can reduce geopolitical and economic tensions. It is counterproductive for national security to impede global connectivity.
4. adopt more measures like mitigation agreements, LOAs, NSAs, and foreign ownership limits as opposed to just blackballing countries, participants, carriers and manufactures.
5. adopt robust third-party testing of foreign equipment rather than blackballing.
6. create more tech driven solutions; develop new open and transparent technologies like OpenRAN, which can really reduce a lot of the fears on third party espionage and sabotage.
7. recognize that individual companies, whether they be Huawei, ZTI, Hengtong, Nokia, Ericsson, IBM, or Cisco, are inherently multinational entities and do not necessarily act the same way than their home countries.

Gary Shapiro contradicted the idea of telecommunication just being a neutral player by referring to human right abuses in China. These are not the values the Western world stands for in terms of human rights and liberty, democracy, the right to religious freedom and the freedom of speech. China putting rights of access to the Internet is a Chinese wall so people can't access news and information. There is a fundamental clash between world views and it is enabled by telecommunication which is being blockaded by China.

Andrew Lipman agreed that these are very critical issues, but considered that there are other ways, diplomatically and politically, to pressure countries who abuse human rights. Creating separate Internets might only reinforce the practice to block information. Only an open Internet could have such a bottom-up popular approach that it would put pressure on some of those foreign governments to lift restrictions and lift barriers. It might be counterproductive to use telecommunication as a tool, where governments or the UN have more effective tools, rather than balkanising the Internet and telecom industry.

Jean-Pierre Bienaimé commented [via chat] that, on the one hand, we should avoid as much as possible to fragment the global harmonisation of telecoms. On the other hand, we cannot ignore the 2019 law in China, that obliges any Chinese company making business abroad to answer confidentially any government's request justified with national security. This explains, for instance, the Western policy towards Huawei.

Sarah Zhao added that technology is like a tool—it can be used as a hammer to destroy or to build something. Using the tool in the positive direction may enhance the mutual understanding of countries and make them do better policies; using the tool for destroying something can make the communication even worse.

Sherif Aziz added that the Internet and digitalisation have been considered as tools for empowering people. However, several Asian regions, not just China, put restrictions on the Internet. The technology is now longer the issue, but how governments are using the technology.

The participants appreciated and enjoyed the lively debate. As the real world is becoming more and more complex and requires knowledge and opinion sharing, such debates become increasingly important. And this is certainly the purpose of the Global Forum: The Global Forum is a place of respectful debate with a view to establish some shared common understanding.

Sylviane Toporkoff emphasized the Global Forum's importance as a place of respectful debate, collaboration and cooperation to exchange views on issues that matter – issues where there is not always an easy answer. In this context, it could be of interest inviting a Chinese representative to further exchange on these questions and to learn about the Chinese perspective.

Alan Shark commented [via chat] that it is not a technology issue. The U.S. has a completely open telecom system, nevertheless 35 million people believe Trump won the election. Our policies are what needs to be addressed regarding social media.

Jeremy Millard agreed [via chat] that governments have a huge role, but no one has mentioned the role of big tech (e.g., Facebook, Google, etc.) who are ruthlessly using the Internet and the monopoly position to enable conspiracies and untruths to be spread just in order to make a buck. So, it's not just a government led surveillance society such as in Russia or China, but also the move to surveillance capitalism (cf. Zuboff).

Lara Srivastava agreed [via chat] that surveillance capitalism is a big threat. The choice is to either let governments control big data and individual identity, or big tech whose only incentive is to distract us (attention economy) and modify our behaviour for their monetary gain.

Jean-François Soupizet, Senior Advisor to Futuribles International & Independent Expert, Paris, France, **shared some remarks on recent trends in the regulatory sphere in the EU**:

Unlike telecommunications infrastructures and the Internet, content, applications and more generally uses in the digital world are not subject to specific regulations and this for two main reasons: on the one hand, it has long been accepted that the provisions governing the real world are applicable to the virtual world, mutatis mutandis, and that there was no need to create a specific law, on the other hand the idea of regulating the digital sphere was strongly contested because of the risk of penalizing innovation, an essential element in the growth of a sector which holds so many promises of job creation and wealth generation.

Today the information space is a reality it is a success that many citizens benefit from in their daily lives. At the same time, many citizens may feel disillusioned by the reality of the digital transition: Never has the concentration of wealth in the hands of a handful of dominant players been so important, never have the prospects of a state or private surveillance society appeared closer.

And it is clear that these transformations are closely linked to the economy of online platforms. The success has been such that the most important of these platforms have their users in the billions and that the data they hold has grown in the same proportions to the point that they have become monopoly players in their initial activity and able to extend their supremacy far behind.

Such a concentration of powers carries with it the possibility of abuse and it raises the question of the legitimacy of the decisions taken by their bosses as illustrated by the “Hamiltonian Momentum” of January 8, 2021 during which the President of the United States was literally cut off by the main social networks active in the country.

This clearly shows that the reasons why the sector had been poorly regulated are now obsolete. And more fundamentally, the scale of the impacts of this new economy poses threats to the economic, social and political stability of our democratic societies.

It is exactly why the EU’s ambition consists in organizing the information space according to rules equivalent to those which prevail in real space and this in conformity with its values. In the last years, measures have been adopted in matters of protection of the privacy of citizens, consumer protection, fair remuneration of authors and creators with the Directive on Copyright and that on Audiovisual Services and the Media and finally it has taken measures about terrorist content online.

But the platform economy largely escapes these measures and in December 2020, the European Commission presented two new proposals, the Digital Services Act (DSA) and the Digital Market Act (DMA). The objective is to structure the “informational space” in order to protect the fundamental rights of all service users and to establish a system of equal treatment between actors to promote competitiveness, innovation and growth in the EU market and globally.

Regarding services, the DSA would cover intermediary services, hosting, marketplaces, search engines, etc. by imposing not a control but a set of obligations concern the means implemented to fight against illegal content and the reactivity of platforms. Additionally, a system of trusted flaggers would be implemented as well as a network of competent authorities at national level in the EU. Finally, vertical provisions would be taken on hateful, discriminatory content, calls for violence or harassment on the model of what exists for child pornography or terrorism.

Regarding markets, the DMA approach is inspired by the experience of telecommunications with asymmetric obligations imposed on players benefiting from market power and for those who control access to market (gatekeepers). These obligations will relate, for example, to the prohibition of discriminating against third-party producers in favour of the services offered by the platform, on interoperability obligations or the obligation to share data provided or generated by the user.

The legal basis for these provisions is in relation with the EU Internal Market and as such they will enter into force as soon as they are approved by the European Council and Parliament, possibly by the end of 2021.

Gérald Santucci commented [via chat]: As for our “democratic society”, aren’t our today’s societies less convinced by the benefits of democracy? What seemed inalienable some years ago, esp. after WWII, is today challenged by many countries, groups, and individuals. The Global Forum could explore the causes and consequences.

François Belorgey commented [via chat]: Why doesn't the EU do anything against blatant monopoly abuse by platforms and marketplaces? Apple and gaming: why no quick reaction? Why the initial version for an EU privacy directive was coming from Microsoft? Cheating and greed has become the norm, with applause. Why not stopping unfair competition as far as it is outside Europe, operating in Europe?

Gérald Santucci explained that it is not easy to react quickly on a topic that is so complex and requires intensive discussions among 27 countries with different opinions and constraints.

Coming back to mobile, he suggested to discuss not only 5G but also the 6G with new frequency ranges, new infrastructure, integration of air-ground-sea and space communication technologies. 6G will boost IoT at all levels, in all spaces, for all applications. It would be great to start a conversation within the Global Forum between the U.S., Europe, China and others.

Jean-Pierre Bienaimé commented [via chat]: 6G should be mentioned in the conference, but not developed at this stage: True and full 5G will not be standardised until mid-2022, with a commercial launch of products and services in 2024.6G will be developed and defined within the 10 coming years; it would be premature to promote it at this stage.

Rob van Kranenburg shared [via chat]: link to “Future Urban Smartness: Connectivity Zones with Disposable Identities”, van Kranenburg R. et al. (2020). In: Augusto J.C. (eds) Handbook of Smart Cities. Springer, Cham. https://doi.org/10.1007/978-3-030-15145-4_56-1

Concluding Remarks

The moderator, Ingrid Andersson, together with Sylviane Toporkoff, thanked the speakers for sharing their precious thoughts and expertise. The topic of the Global Forum 2021 is strongly connected to the current global challenges and some important issues have been touched upon today.

A big thank you to the participants for bringing up so many interesting points and the very inspiring debates—because this is what the Global Forum is about: creating room for sincere discussions and constructive debates on issues that matter in shaping the future.

The moderator reminded the upcoming two webinars:

Global Forum Thematic Webinar II on April 7th, 2021

- "COVID-19 Pandemic as a Science and Technology Accelerator?"
- "Disruptive Digital Technologies, Artificial Intelligence, IoT, 5G, Blockchain …"

Global Forum Thematic Webinar III on June 9th, 2021

- "Industry 4.0"
- "Sustainable Smart, Cognitive Cities, Regions & Communities and Tech for Good"

The participants agreed with the timing of the webinars: 1:30 pm to 3:00 pm Paris time / 7:30 am to 9:00 am Washington DC time / 9:30 pm to 11:00 pm Tokyo time.