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

TOPIC 2

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

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

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

Questions & Answers

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.

Comment/ Question 1: 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.

Comment/ Question 2: 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.

Comment/ Question 2 : 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.

Comment/ Question 3: 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.

Comment/ Question 4: 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.

Comment/ Question 5: 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.

Comment/ Question 6: Agreed 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).

Comment/ Question 7: Agreed 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.

Comment/ Question 1: 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.

Comment/ Question 2: 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?

Comment/ Question 3: 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.

Comment/ Question 4: 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.

Comment/ Question 5: 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