"Splinternet" – Danger for our citizens, businesses and society?

Once upon a time, there was the World Wide Web (www). Just as it was invented by Sir Tim Berners-Lee.
John Perry Barlow wrote the "Declaration of the Independence of Cyberspace" in 1996. The Internet was a great promise of freedom. It worked like a continuation of the Gutenberg invention, the printing press: the Internet gave a voice to all citizens whose views and attitudes were suppressed by the media and elites. This had and has great political consequences.

30 years later the opinion about the internet changed: It was thought that monopoly companies like Google, Facebook, etc. control Big Data and Artificial Intelligence, and therefore control us. However, politics followed suit and began to regulate. The concern now is that the state will disenfranchise citizens and restrict companies. There is a fear of new totalitarian regimes.

And in this situation, the Internet ("splinternet") is increasingly fragmented. National "Internet" networks are emerging. States treat the Internet as an extension of their national territory. The most recent example is Russia, where Kremlin laws ensure that national Internet traffic goes through state nodes and the state has the right to shut down the global Internet: a sort of digital Iron Curtain. The champion of the national Internet is China. The state monitors and controls Internet content, blocks foreign services and companies (like Facebook) and replaces them with national services and companies that are in line with the Communist Party. The "Great Firewall" is successful. The number of states imitating China's Internet policy is growing: Iran, North Korea, Cuba, Turkey, Saudi Arabia, but also Thailand and Vietnam etc. have introduced laws that allow them to control and censor "their" Internet.

Three main approaches can be observed with the "splinternet" when replacing the global Internet with regional Internet:

	Europe	USA	China and imitators
Goal	Protect people	Empower people	Control people
Approach	Heavy regulation (eg GDPR)	Light regulation	State dictates
Economic impact	Older Industries Protected	Disruptors Dominate	National Champions Dominate
Societal impact	Seeking middle ground	New voices empowered (Wild West)	Social Credit Scores

Source: Bruce Mehlman

Europe's approach to protecting the privacy of individuals is primarily through the basic data protection regulation, but also through the commitment of tech companies to store European data exclusively in Europe and to delete information at the request of citizens (worldwide). Sir Berners-

Lee's SOLID project aptly characterizes the European vision of the Internet: SOLID should enable users to control and securely store all personal data themselves.

It is striking that the West is also pushing the "splinter Internet": In Europe, companies have to be compliant with regional and EU laws when using data on the Internet in each country, and regional storage is increasingly required for data storage. The location of the company's headquarters as a central criterion for taxation is also being questioned for Internet companies. The establishment of a regional Internet infrastructure (such as RUS or CHN) is also being discussed. The "Western model" is thus already fragmented in itself. On the other hand, American companies are increasingly blocking European users from their websites in order to avoid having to comply with European data protection guidelines.

The common denominator of the West is probably the commercialized Internet, a marketplace for inventing and improving business and increasing productivity for the benefit of citizens. How open this Internet must be, what content must be accessible to everyone, what may be published - here the "Western minds" are already divided.

This Western system, which is already struggling with internal frictions, is confronted with a compact Internet model of Chinese character: The state must control the Internet and therefore its citizens - so that the authoritarian state can cement its power.

It is difficult to imagine that these different "Internet" will find common governance or even return to the roots of the Internet idea, to the free Internet. The fear that citizens will lose their freedom with the help of the Internet has a concrete face with the China model, with social credit scoring, with the persecution of dissidents via the Internet and social media. The promotion of state champions by keeping the competition at bay and the rule-free use of citizens' private data (with 100% system loyalty in return) has also become a point of conflict. Huawei is the synonym for the fact that it is only a matter of time before the symmetry in competition with Alibaba or Ants is called into question by the West.

On the one hand, the Western Internet, defends its freedom over large areas. Where one can imagine that a common governance will be found. On the other hand, the state internet, is used to control its citizens and (with asymmetrical rights compared to western competitors) to create national champions.

Can we (the West) afford to offer authoritarian states, which control access to information and opinions, all our information, all our knowledge via the Internet, so that regimes can freely choose what is useful for them to control their citizens and strengthen their economy? Shouldn't we rather fear that our personal data and opinions will find their way into the information monopoly of authoritarian states? IT infrastructure, (all) social media and payment transactions? With the consequence that we, once identified as a

system-critical person, can no longer travel (visa), or even worse, we can enter authoritarian countries but cannot leave!

The western, democratic and free world cannot actually accept an Internet that serves to control and incapacitate citizens. Not only because it threatens us too, but because we have a duty to work for the freedom of all peoples.

Can the Internet of western design prevail with the help of the market and technology? For example, through the Internet of Things (IoT), which is an opportunity for Europe to set global (market) standards. Or through encryption technologies as a strategic export article of the USA? Or are we at the mercy of risks if encryption is compromised by quantum computers and we cannot guarantee security in IoT: So not knowing who is driving my car, my refrigerator, or my power plant. In any case, politics is called upon to protect our freedom!

For politics to be effective, the "Western Internet" must first find a common governance - to be able to speak with one voice. It seems essential that we agree on how the constitutionally guaranteed freedom of opinion is defined. So that it is and can remain the highest good on the Internet. Only in this way will the Internet contribute to citizens' freedom, vitality and the productivity growth of the economy. Productivity growth that makes life better for all citizens and makes our democratic institutions work.

We wish you a successful 2020 !!

Dr. Hannes Enthofer Patrick Haas
Partner Finance Trainer

Luxembourg, 31.12.2019