THE TRANSFORMATION OF GLOBAL GOVERNANCE PROJECT

25-26 NOVEMBER 2019 SEMINAR

THE GOVERNANCE OF DIGITAL NETWORKS: CONVERGENCE OR FRAGMENTATION?

Seminar insights from the organisers

G. Hammerschmid, P. Howard, G. Papaconstantinou, J. Pisani-Ferry and D. Stockman

1. **The governance of digital networks has unique characteristics.** The relationship between global governance rules and actual interconnectedness in different fields is not straightforward. From an initial state of near-autarchy, for flows to develop between islands, or in some cases as flows developed, rules were put in place to govern them. Rules were defined early on in the case of trade and the global financial safety nets, more or less in real time for competition and banking, later for taxation and climate change mitigation, and almost not at all for migrations. In the case of digital networks, things developed differently; interconnectedness came before state-sponsored international governance rules. The network was the brainchild of a transnational community (the scientists). It was born global, and nations caught up belatedly.
2. **The pendulum is swinging and the demand for governance rules is growing.** Across many policy areas we observe today a move away from traditional rules-based multilateralism towards variable geometry approaches to global governance, reflecting a more polarised and fragmented international environment. In digital networks the reverse has happened. Initially, their governance was meant to be light, open, participative. The US supported this approach as it promoted its geopolitical outlook and buttressed the predominance of its companies. Developing countries fought against it in the early 2000s and lost. But today the pendulum is swinging in the opposite direction. The multi-stakeholder model is still dominant, but states (in developed and developing countries) are now attempting to reassert some control.
3. **The different layers of the internet complicate its global governance.** The internet is elusive because it consists of several successive layers that cannot be considered separately: physical and logical architecture, services and data. The physical architecture is basically made up of telecom infrastructure. Its evolution involves an economic question (whether telcos and other players have sufficient incentives to maintain and develop it as volumes and costs grow exponentially) but also involves a strong security dimension (this is the core of the whole discussion about Huawei). The logical architecture - the core feature of the internet - was born resilient for security reasons and has retained this property, but its evolution involves an issue of its control and utilisation in conflict situations. The dedicated services layer is increasingly cartelised and dominated by the response to the particular business models of these cartels. The further level is that of the data dimension and covers the whole economy, from cars to insurance and finance. In addition, there are important spillovers across levels, e.g. from dedicated services to infrastructure and to general provisions regarding data exchange for all sectors.
4. **Security, privacy and competition concerns are driving the debate**. As the internet developed and became the backbone of information exchange, several things happened. First, its use as a conduit for malicious initiatives by criminals or foreign powers grew. Security dimensions became major and led states to reassert their sovereignty. Second, long-standing differences in national preferences as regards privacy and free speech emerged as strong forces of fragmentation along national lines. Third, tech firms fragmented the internet further by developing specific semi-open or closed networks. States in turn started to attempt to regulate these networks. Competition

now is between these alternative forms of fragmentation. Accordingly, and following these changes, the debate about governance has been driven by different perspectives: a security one, focusing on infrastructure; a perspective of human rights, focusing on privacy; and an economic one, centred around competition and regulation. These often converge, but have fundamentally different starting points and characteristics.

5. **Cooperation on infrastructure governance is not up to the challenges at hand**. Digital networks are vulnerable and the potential for malicious security breaches (or unintentional failure) ranges from a localised problem to a global catastrophic system break-down. Nevertheless, and perhaps because a major disruption has not yet occurred, few rules have been agreed upon as regards security in cyberspace, beyond a vague commitment to preserve the core architecture of the internet (which is probably in everyone's interest, except North Korea and a few other rogue states). The persistent engagement doctrine followed by the US is in itself an obstacle to further codification. Current private and state engagement and commitments fall far short of what is required in the emerging mixed polycentric model of infrastructure control. They need to be developed further in both infrastructure and services, combining both technical and legal safeguards.
6. **Fragmented preferences and the dominant business models hinder tackling privacy concerns**. Differing attitudes and preferences are a factor in the governance of many policy areas. In digital networks, US-style "surveillance capitalism" built on the business model of the tech companies has combined with sophisticated Chinese state control of networks and data to squeeze out concerns about privacy. While self-regulation has proved woefully ineffective, some initiatives have broken new ground: the European GDPR has proven successful legally beyond EU borders, even though its effectiveness has not been fully tested yet. It is based on a legalistic model rather than on a supervision model, and initiatives of this type are bound to trail technical developments. There is a need to move to a supervision model that relies more on principle-based regulation, transparency and accountability. This may be the best that can be done, short of an outright ban of the business model of providing services in exchange for users' data that the networks rely on.
7. **Competition conditions in digital companies and platforms need to be strengthened**. Abuse of dominant position, creating barriers to entry, and capturing a disproportionate part of the value generated by users characterise US tech giants and increasingly their Chinese counterparts. Making digital markets that enjoy large network effects and economies of scale and scope contestable and contested in practice through competition policy and regulation is difficult. This is due to fragmentation of preferences as well as the characteristics and sheer complexity of the digital sector (scale without mass, complex value chain and products/services), obscuring the relevant market for competition policy. Notwithstanding the difficulties, strengthening competition conditions is increasingly a matter not just of efficiency but also of democracy. It should be based on principles of non-discrimination, separation and access, build on the experience of telecoms, while not excluding separation of activities.
8. **A way forward through principles, rules and bold initiatives**. The multi-stakeholder model that has nurtured digital networks has run its course; to be saved, it needs to be reformed. This involves principles, rules, and some bold initiatives. The momentum towards legal pluralism and fragmentation is probably irresistible, but some commonalities ought to be preserved. They should consist in a series of "don't do", mostly regarding security, coupled with broad common principles that could play an equivalent role to that of the WTO basic rules. They should essentially address issues related to extraterritoriality and help determine the legitimate reach of the various jurisdictions. It could also include an IPCC for the data-driven world where scientists share knowledge and formulate joint recommendations, and a stronger role for fora based on multi-stakeholder culture. Finally, competition policy should include a re-examination of the business model of digital platforms as well as of the scope of activities of dominant tech giants.

Keynote by Caroline Atkinson, PIIE

Some hard questions of digital governance

Digital governance faces difficult questions of defining what is to be governed, and how best to do so. Five important policy issues can be discerned: competition; content; copyright; data and privacy; and AI. A sixth, issues of tax, could be added, but it does not pertain predominantly to digital governance and thus need not be recalled further.

1. ***Competition**. Economic power determines competition conditions. These hinge on the definition of the marketplace and its actors, and sovereign decisions that take effect if the scale and internal cohesion of one actor compels others. While the US still has the upper hand, the EU possesses this critical mass and is capable of skilled decisions in this, but is limited by its stunted digital single market. The large digital, platform and tech companies — Amazon, Apple, Facebook, Google, Microsoft and Netflix, to which must be added the Chinese giants Baidu, Alibaba and Tencent — now also wield extraordinary economic power. This translates to other forms of power: they touch people's emotions. They evoke utopia through the products and services they provide, their low-to-inexistent cost, and their convenience; but also dystopia, though their abuses and inescapable ubiquity.*
2. ***Content**. Laws regulating content exist where they do, and are enforced where they can. "Mechanical Turk"-style content regulation by human hands is the consequence of the increased demand for effectiveness and speed; efficacy remains lacking however. Harmful content and disinformation are a user-generated problem; while platforms share blame in its spread, it is not tenable to put responsibility for content selection solely in their hands. Content regulation is more naturally the purview of governments, though liberal values should be upheld to the greatest extent.*
3. ***Copyright** and intellectual property are more intangible even than the digital world, and lie at the heart of many of its governance issues, material and immaterial. Democratic societies can have differences of conception, enshrining different choices and values; but democratic choice is easily vitiated by lobbying with special interests and deep pockets.*
4. ***Data and privacy**. The value of data lies predominantly in its aggregation and monetization to target advertisements. Thus the problem lies more in the governance of advertising, not just its digital aspect. Targeting advertisements implies a form of surveillance, the continuance of which can only be a political question and subject to the development and legitimate expression of preferences within different polities.*
5. ***AI** once seemed to promise that furthering machine learning with data would teach intelligence to teach itself, in order to solve all problems. This naïve view is giving way to a clearer vision of what AI can and cannot solve; it has already led to a revolution, if not the promised one, and is still ongoing and unpredictable. Companies have underestimated the policy dimensions of what they have unleashed, taking more of an engineer's view of what people want and need and how to supply it.*

Policy-makers should aim to first do no harm, but decisions will entail trade-offs and democratic balances to be struck; for example between privacy and law enforcement. In these decisions, it is important to understand where interests overlap and represent all stakeholders. Similarly, at the international level, like-minded (and powerful) states can identify overlapping sets of interests, get political commitments, and obtain high-level agreements to produce governance. Private actors, expert communities, and policy actors should engage in much more dialogue to shape the way forward.

Fragmentation fears are in large part due to the relative situations of the US and China: political ontology aside, both have huge and powerful digital companies, and both have security establishments that are deeply distrustful towards each other. While the Huawei issue may be more geo-economic in nature than one of foreign intelligence, Chinese actions (Hong Kong, Xingjiang, South China Sea, the Social Credit system…) do not reassure. Cooperation could begin on a lowest common denominator of combatting cybercrime, agreeing to sanctuarise critical infrastructure, and offering mutual aid in case of emergency. In parallel, liberal democracies could band together and co-regulate with companies, working for example on freedom of data flows.

Companies can help their case by responding to citizen dissatisfaction, working on their data policies and leaving tax havens. They should be more transparent on their content policies, countermeasures, income and activities. Issues of political advertising may just be the old problem of money in politics combined with the new one of microtargeting through surveillance capitalism. Resources should be directed at disinformation and abusive content problems . Companies could shed pieces of themselves, but it is not a single fix and cases should be considered in their specificity; speaking of digital companies collectively obscures their internal competition and different specialisations. They must also sometimes walk a fine line with what governments task them with or ask from them.

Main discussion points from the seminar

Session I – Digital governance in the broader global governance framework

The first speaker introduced the session by evoking the patterns that disruptive technological innovation leaves on society. Its introduction is initially not considered important or of regulatory relevance; but then, when its societal or economic impact becomes clear, there follows a second stage with a push for regulation, motivated by a concern to protect citizens' rights or space for corporate innovation. The still-developing technology is a moving target for regulators, however, and when it is fully integrated in society it may become clear that some measures have become obsolete or were fundamentally misconceived. Rules such as interoperability clauses follow in a third stage.

"Digital governance is both a blessing and a curse, because it's so wide."

Regarding issues of digital governance, the global community is in the second stage. This raises the question of what role to allocate the private sector in co-creating governance while protecting citizens. Whereas governance has long been the task of states (and recently international organisations), private regulatory actors (and to a lesser extent civil society) have a genuine impact on governance that calls into question traditional checks and balances. Institution such as the EC/OECD/UN all propose the stimulation of private regulation; but the role of private actors and of civil society is not clear. There is hope they may supplement the rule of law, and fear they might replace it.

The second speaker recounted a brief history of the expanding relevance of digital governance, which started initially with the coordination of names and numbers, and then moved to work on issues of the information society. The World Summits on the Information Society in the early 2000s reflected concern amongst governments about the US dominance in the field, among others through its grip over ICANN; increasingly prominent attacks and criminality through cyberspace later in the decade brought the imperative of cybersecurity to the fore. Today, the digital world intersects global governance in three areas: trade, with the development of e-commerce; security, which may be the most consequent; and, mixed with security, content regulation, following the experience of disinformation campaigns targeting democratic processes.

Responses to these challenges, consisting in attempts by governments to establish jurisdictions and borders in cyberspace, have been framed as a "fragmentation" of the internet, but this is incorrect

according to the speaker. Secession of a sub-system is not an unprecedented possibility, nor does it imply technical breakage. A better characterisation would be an “alignment” of cyberspace to sovereignty conceptions, though it would be preferable (and more suited to its nature) for the internet to be preserved as a global commons.

In the ensuing discussion, one participant disagreed strongly with the second speaker, arguing that without sovereignty we do not have democracy. After being on the side-lines for too long, many states are appointing digital ambassadors and getting more politically involved in governance structures to defend their interests in response to their citizens' needs and demands. Conversely, some companies are sending "ambassadors" to relevant international organisations.

While the focus has been, and should continue being, on how public actors can protect citizens from exploitation by private actors, it was suggested that upholding certain rights of moral persons can also protect human persons from governments should not be neglected. While it seems that concepts of classical international law can be applied to cybersecurity and threats to digital infrastructure by belligerent states and transnational crime, the conversation about their updating and implementation is ongoing. It is unclear what role the private sector is willing to play: many large digital companies are now calling for some kind of regulation, both to be guaranteed some kind of clarity in order to conduct their business and to defuse some of the popular backlash against them. This call can be considered hypocritical, given their lack of forthrightness in effectively cooperating. The optimal extent of infrastructure privatisation is in question, as renationalisation is beginning to take place, while some private actors are setting up their own infrastructure.

“Digital diplomacy is not only about regulation; it is also about rights and economic development”

The spread of harmful content however requires active engagement with the private actors who host it; while there is convergence on the most egregious types of content (i.e. terrorism), ceding too much power to private actors runs the risk of unaccountable and undemocratic "rule by algorithm". Less egregious content (hate speech, disinformation) is more complicated. Against the original libertarian ethos of the internet, many feel that some kind of rule of law should apply, not just a maximalist and extraterritorial interpretation of the US 1st Amendment.

In fact, it was argued that a large part of content does not fall under its purview and can and should be regulated as corporate speech, under its form of paid advertisement. It may be that the business model of providing "free" services in exchange for personal data is itself harmful: social networks are designed to capture the attention economy, promoting and selling advertisement of sensationalist content to force more engagement and extract more data. Moreover, content regulation by corporate AI is an illusion as it needs to be trained and maintained by human input, with insufficient effectiveness and considerable psychological damage to these workers.

The GDPR has established data governance in the EU, despite predictions of economic catastrophe and huge lobbying efforts against it, though its problems must be faced with clarity. It also seems to have managed to establish minimum privacy standards worldwide, due to the scale effect of the EU market. One participant contended that the effectiveness of its obligations (privacy by design) and sanctions has not been truly tested yet. Talks are ongoing at the G7 and G20 level to balance its requirements with the need for free data flows and ensure the digital commons do not suffer enclosure, though these talks may be lacking in concreteness. The OECD is leading an initiative on AI governance, taking the IPCC as a template for multi-stakeholder knowledge production. In this context, it was considered unfortunate that the WTO is crippled and cannot serve as a forum for these issues; even more so that responsibility for governance is so fragmented across international organisations.

The discussion made clear that what is at stake is governance of many issues (some new and some not) undergoing changes due to digitalisation, rather than the governance of digital issues per se; cyberspace is another means through which economic distortions can spread. Material issues (i.e.

infrastructure) cannot be easily sifted out from immaterial ones (i.e. content), as they interact and interpenetrate; traditional international relations are ill-equipped to deal with these because they are fundamentally grounded in territoriality. Both infrastructure (e.g. Huawei) and digital applications (AI) can carry and embed preferences or societal models. The view of cyberspace as a commons was disputed; a better metaphor may be that of a condominium, with both private and common spaces.

The speakers concluded by putting the theme of fragmentation in question: different states have different value sets, but interconnectedness ensures that every action affects every actor (sometimes with aggressively hostile intent, as with Russia). All actors must be brought together to co-create regulation, especially the private sector and expert communities (regulators and academia).

Session II – Internet infrastructure and national security

The first speaker presented the case of Estonia. The government has been offering digital services on platforms developed through public/private partnerships since the mid-1990s, building a backbone of digital infrastructure and exporting its solutions internationally. This choice has entailed risks: a 2007 denial-of-service attack (traced to Russia) paralysed vital services and is notorious as one of the first large-scale geopolitical cyberattacks. Yet, trust in Estonia's digital infrastructure and services (including voting services) remains strong.

As digitalisation continues to progress globally, three ideal-typical scenarios can be distinguished: the development of platform ecosystems controlled more by private actors, by governments, or in a mixed fashion. Each carries different risks. The private option runs the risk of domination by US and Chinese companies (and the underlying values behind them, as well as their governments enjoying more or less control of them). The governmental option runs the risk of splintering cyberspace, increasing security at the expense of openness and the potential to harvest greater network effects. The mixed or polycentric option has the advantage of robustness, but the disadvantage of more complex governance.

"It's not the internet that's broken; it's us."

The second speaker (Marsden) countered that Estonia may be the exception that proves the rule. Malicious content and disinformation spread at little to no cost across platforms such as Facebook or WhatsApp has perturbed elections in the US, the UK, Brazil; fuelled violence in Myanmar, Thailand, Kashmir; an election had to be entirely rerun in Kenya. This content is not the sole cause of the outcomes, but it has very tangible effects. Content regulation by corporate AI is a wild goose chase; governments are not paying enough attention to expert and electoral commission recommendations.

The third speaker focused on the question of how to build long-term stability. While conversations are taking place among a usual group of experts in digitally-oriented forums (i.e. the IGF), they have yet to reach those forums dealing specifically with security issues (i.e. the Munich Security Conference). There has not yet been a "cyber 9/11" or a "cyber Pearl Harbour" with mass casualties, though cyberattacks are becoming more prominent, and IOs and civil society seem more cognizant than states of the necessity to act. The UN Global Commission on the Stability of Cyberspace has developed principles akin to those in the Geneva Conventions on war (prohibiting attacks on critical infrastructure, distinction of the enemy, proportionality of response…), but accountability and effective consequences are still quasi-absent; although the US and the EU are starting to devise ways to do so under some kind of framework beyond current military intelligence activity. Trust can be built through emergency communications and de-escalation mechanisms, but this remains bilateral; collective action responses are impossible to build given the unilateral and extensively "extraterritorial" cyber-response doctrines of some countries (i.e. the US' "persistent engagement" strategy).

The relation between sovereignty and military cyber-response doctrines was discussed: it cannot be overlooked that the origins and destinations of attacks are indeed territorial, but since they are

mediated by non-territorial cyberspace, calibration of their attribution and deterrence is much more difficult. "Rules of the road" in cyberspace should not be set tacitly through cyber-response doctrines, but explicitly and in non-military forums; though sometimes unilateral elimination of a cyber-threat can be appropriate. There is a worrying ignorance or acceptance of the current vulnerability of large parts of states' infrastructure (including financial or energy infrastructure) compared to concerns over disinformation attacks. Against malicious actors that foster "hybrid" threats, clarifying responsibilities for attack and defence regarding infrastructure and content in states' defence structures can be helpful.

One participant recalled that threats don't only originate from malicious actors, but also human error and natural disasters. Japan came close to a complete internet blackout due to the 2011 earthquake and tsunami: safety backup systems should be put in place, like those built in settlement systems for finance. Another argued that cybersecurity by itself is not enough, pointing to the need for legal security as well. Estonia maintains a "data embassy" in Luxembourg, a mirror of all its essential governmental functions, with the legally protected status of diplomatic premises. A third participant responded that such an outsourcing of sovereign functions is not new, citing the legations of the Estonian government-in-exile during the Cold War, and that effectiveness depends on the recognition of other (larger) states.

"5G is not a technical issue, but a political issue."

One participant distinguished security requirements of infrastructure (highly regulated and scrutinised) from those of the services that use it (much less so), underlining the need for a holistic approach. The concept of duty of care in tort law could be repurposed to encourage (corporate) actors to take on more responsibility in exchange for exemption from some (legal) liability. Discussion on infrastructure quickly centred around 5G and Huawei: one participant challenged the discourse of cybersecurity concerns as a scarecrow, disguising industrial policy as then Ericsson would then be the only viable 5G company in the EU. Another responded that the concern is merely that critical infrastructure should not be the purview of a single company, and that it should not be shaped by the US/China trade war. A third added that while this holds in many countries, this question does not make it into security debates because of its low electoral salience.

One participant countered that this is changing fast, as politicians cannot afford to not pay attention to cybersecurity any longer. Another expressed pessimism as to cybersecurity in politics: it is already difficult enough to mobilise effectively against infrastructure attacks, and content-based attacks have proved orders of magnitude more difficult to deal with. Few had anticipated these kinds of attacks, and much more information is needed to study them: it is imperative that platforms share their data on this, but they are extremely reluctant to cooperate.

Session III – New competition concerns

The first speaker in this session spoke to the problem of sharing the value captured disproportionately by digital companies and platforms, generated mostly by their users, in what can be considered an abuse of their dominant position. Better regulation presents a huge challenge due to the network effects that allow them to enjoy self-reinforcing economies of scale and scope, rooted in their use of larger amounts of data, and mediated through an increasing number of intermediary actors along the value chain. Competition policy and legislation will have to be deployed to secure competition, transparency and wider democratic values, and it is in platforms' interest to accept and pro-actively support regulation to begin to earn trust back.

"Digital markets must be contestable and contested."

"Significant" platforms, analogous to EU critical infrastructures or G-SIFIs in the financial and banking sectors, should be monitored since they function as the "gatekeepers" to digital markets, though the criteria for determining this status remains unclear. Flourishing competition can be

fostered by principle-based regulation: for digital markets, classical principles of non-discrimination, separation and access should be upheld. In all there is a need for better alignment of data protection, competition, consumer protection, and regulatory measures; but the only way a governance arrangement that rebalances power relations can be set up is through law.

The second speaker focused on the interaction between trade and digital governance, highlighting three competing sets of interests: commercial (uninhibited data flows and little regulation); individual (privacy and personal rights); and governmental (national security and law enforcement). The ideal forum for debate on balancing these would have been the WTO, but it has been paralysed on this issue for two decades as technological progress has only accelerated. As things stand, the world is divided into three "digital kingdoms", deriving rules from domestic law and FTAs or plurilateral agreements. In the American kingdom, free flows of data with little to no localisation or privacy requirements are preferred, and are actively promoted through trade agreements. In the European kingdom, privacy and personal data rights are preferred, and made effective through extraterritorial application of its law, as attempts to do so in trade agreements has not been a success. Finally, in the Chinese kingdom, a form of "cyber-sovereignty" that rejects free and unlocalised data flows as well as strong privacy protections is preferred, though its legal codification and the bodies to enforce it are quite recent.

These preferences stem from different commercial interests: the US has more interest in dematerialised services, China in physical goods, whereas for the EU it is "e-protectionism" though its GDPR. They also stem from different values and regulatory philosophies: light-touch self-regulation for the US vs heavy governmental intervention for China, as opposed to a strong focus on human rights for the EU. These differences notwithstanding, competition issues are global issues; the WTO reference paper on telecoms could provide a basis for the necessary global rules.

The third speaker spoke to the properties of digital industries that make it difficult for policy to capture their actions and effects. They display an unprecedented profile of scale without mass (with high fixed and low marginal costs) with a panoramic scope and complex products, which obscures the relevant market for competition analysis. Their speed, as well as the iterative experimentation it allows, are also unprecedented; this leads to winner-takes-most dynamics where dominance due to weak competition is difficult to distinguish from that due to a "superstar" effect benefiting established actors. Their source of value is intangible, based in establishing quasi-monopoly rights based on their exploitation of data and massive investments at a loss to drive out competition and corner the market.

"Data is not oil. It is not rivalrous like oil; though it has comparable externalities…"

Accordingly, the market has been less dynamic, with fewer entrants, since 2000, while mark-ups and aggressiveness in M&As grow. Policy has hung hopes on data portability to ensure greater interoperability and lower barriers to entry, but this has not materialised, and may be technically unfeasible. A more radical solution might simply be functional separation, based on the telecom model. As non-tech industries increasingly adopt a platform model (i.e. heavy equipment manufacturer John Deere), the question remains how to establish a global regulatory regime that also includes China. Chinese digital companies are barely a decade old but have acquired enormous market power, if limited outside of the mainland; unlike Western ones, they already include a payments system.

One participant suggested that, however difficult it may be to define markets and remedies, the structural power of the large digital, tech or platform companies makes them inevitable candidates for regulatory experimentation. Another objected that it seems these companies are held guilty a priori, and that users are "willing victims", bartering away their data to enjoy digital products and services made possible only by the network effects these companies create and maintain; regulation may create just as serious distortions and failures as markets can.

The first speaker interjected that governance is such a problem in this field precisely because of the great value produced that users cherish and that drives growth and innovation. Tirole's advice to require proof of benefits rather than proof of no harmful effect in M&As, hearkening back to earlier practice in antitrust, could be a useful line of thought. One participant reported that the EU will be reviewing its definitions of relevant markets and state aid, while moving towards a proactive digital industrial policy to further its assertive stance. A school of thought that promotes stronger antitrust is attracting attention in the US; China's recent codification of competition laws and institutions is to note, but hope of any autonomy is slim.

One participant agreed that a weakening of antitrust has allowed these companies to grow so large, and drew attention to the fact that some smaller companies' "source of value" and business model were in fact to be bought out by the top-tier companies (e.g. WhatsApp by Facebook), furthering their bundling of services in exchange for ever more data collection (and in the end surveillance, through collation and aggregation). Another noted that such bundling could be considered actionable as a restriction of consumer information and/or choice, but it would be a fundamental challenge to current business models, and would test the limits of the extraterritorial application of competition policy. A third participant raised the spectre of Western and Chinese digital giants collaborating rather than competing, which would complicate matters even further.

One participant drew attention to how these dynamics fuel inequality and how it correlates with political polarisation, making a parallel with early 20th century lack of economic and financial regulation and inequality that led to creating the Bretton Woods institutions at the end of WW2, and advocated strongly for a solution based on taxation. Another participant objected that tax shifting is not specifically a tech industry issue. A third countered that the situation is more complex, as determining tax obligations hinges on determining where the transaction is taking place; this same uncertainty related to defining "extraterritoriality" of actions in cyberspace writ large.

A number of participants called for discernment of the various means to be used to solve the different issues at hand: splitting Facebook with antitrust would not for example solve content issues such as hate speech. Likewise, monetising free digital services would be a revolution, but would not necessarily ensure that data is not aggregated for improper or commercial use. The forum to address all these issues is uncertain: a least-worst option may be the G20, though its lack of secretariat and revolving presidencies makes it difficult to empower effectively; its Global Forum on steel overcapacity has not worked very well, for example.

Session IV – Privacy and law enforcement issues

The first speaker in this session offered a civil society perspective on privacy. Commitments by telecom companies and internet providers can be catalogued and benchmarked; engagement, year-on-year comparisons, as well as the threat of name-and-shame can provide a lever to hold these companies to account. Nevertheless, it was suggested that large parts of their business models are predicated on violating the human right of privacy to sell targeted advertisement, as a form of "surveillance capitalism". This poses serious questions for governance. It is the deeper problem that lies at the root of separate issues of algorithmic and automated decision-making.

These mechanisms create curated information bubbles, reshaping the public sphere and political reality for countless people; their potential for intentional harm through disinformation was amply discussed, but they can also spread artefacts and inaccuracies unintentionally, but with no less malign effect. Still, too much focus is put on these issues of content rather than on the business model itself. It may be premature to break up the big companies, but there is an urgent need for transparency on their internal operations, of what data is being collected for what purpose, to foster accountability.

"It's too easy to fall back on the national… We need more coordination, or we will have a less global internet."

The second speaker spoke on the shortcomings of international cooperation in law enforcement due to multiple overlapping and fragmented jurisdictions and normative orders. Consciousness of these problems has however thoroughly permeated discourse, and there is a sentiment of extreme urgency to catch up with regulation and legislation to deal with these trans-border issues. Mechanisms already exist, such as the US Cloud Act or the Council of Europe's Budapest Convention, but little dialogue between them. Civil society and expert communities can contribute by mapping the ecosystem of existing actors and legal rules and standards, to then develop and propose new and better (but voluntary) ones.

The third speaker widened the scope by highlighting the tension between the two topics of the session: their intersection creates conflicting legal and political demands. Internationally, this is not limited to the US and the EU, though they are the most prominent: Russia and China loom large. Privacy is anchored in and achieves its current "gold standard" in human rights treaties (i.e. the Council of Europe's Convention 108 for the protection of individuals with regard to automatic processing of personal data) and regional instruments (the EU's GDPR) which, despite their flaws and difficulty to hit a rapidly moving target, have had considerable impact, even "extraterritorially". But while there is a trend towards convergence at the higher levels, there remain considerable differences at the national level, due to different standards and preferences.

Privacy enforcement relies more on soft incentives than hard legal action: individual or corporate clients are shunning businesses that don't comply with the GDPR. (This may, counterproductively, put more burden on SMEs than on the big companies, for whom adjustment is just the cost of business.) Law enforcement, on the other hand, touches on core sovereignty functions: some regional success can be observed (Budapest Convention), but large-scale convergence is doubtful. It remains to be seen what governance approach will prevail in managing these issues: top-down "constitutionalisation" through treaties and law, or a form of global legal pluralism that aims to manage differences through regulatory cooperation. It also remains to be seen how these approaches can be fostered, when compromise is so difficult due to such divergent preferences and core values.

One participant challenged the premise that "pluralism", understood as simple acquiescence to fragmentation and only pursuing minimal coordination, is sustainable or desirable; the underlying reasons driving a demand for governance must be critically examined. Another concurred, adding that allegedly inviolate preferences can be instrumentalised to obscure a form of cultural relativism: Chinese citizens want to enjoy digital rights (among many others), just like anyone else. Several participants cautioned though that "preferences" in a broad sense must be taken seriously, as they can unexpectedly sink important initiatives. Unchecked pluralism however leaves the door open to arbitrage and shirking obligations; the stronger regulator may have to accept a trade-off and forgo a certain potential for innovation if encoded preferences do not allow the use or aggregation of certain data with certain others, especially with authoritarian and non-democratic states.

Another participant considered this trade-off perfectly ordinary: its strong version is a siren song calling for a race to the bottom, and doomsayers are habitually disproven; the focus should instead be on creating a race to the top. The EU is working on deep coordination with others (i.e. Japan) and on an umbrella agreement with the US, but there is little hope for a grand multilateral convention or treaty: the way forward is plurilateral, like the WTO's Agreement on Government Procurement. The G7 has initiated a Global Partnership on AI; there is an effort within the OECD to standardise reporting on terrorism and hateful content, following the Christchurch massacre, but the US seems not inclined to be cooperative. China has made proposals on cross-border data sharing, but tailored to its interests.

There was agreement that instruments exist to push forward on transparency and should be exploited more; one participant

"There is no 'exceptionalism of the internet'; it does not do

suggested a proactive litigation strategy. Software can be considered a manufactured product, with similar obligations of due diligence and oversight to other complex and potentially dangerous material products, such as cars. Indexes and benchmarks can prove subtle, though at times quite effective instruments to realign incentives, even for corporate giants. Another participant remarked that while the public, regulators, and governments have little visibility of what these companies are doing, the companies themselves seldom enjoy much more: only existential threats push them to put things in order, so lacking knowledge should not impede regulatory experimentation. Participants agreed that more will and resources should be deployed, but with care; it should be possible to achieve minimal standards.

Session V – Information control and platform regulation

The session chair invited the speakers and participants to think of control of information along two dimensions: that of truthfulness; and of intent to harm. Spreading content of harmful intent with mostly true material is *malinformation*, comprising leaks, harassment, certain versions of hate speech. Spreading mostly false material with little harmful intent is *misinformation*: viral diffusion, due to scale and network effects, can occur with devastating consequences (panics, conspiracy theories), and be weaponised (stochastic terrorism). Content that is both false and malicious is *disinformation*; electoral interference is a salient example. Each may be dealt through different types of regulation.

"Theoretically, we should be in Heaven. It should have been the end of History. But these tectonic shifts have had bitter side-effects."

The first speaker discussed the sometimes surprising effects that platforms have had on how information spreads and is received. Social media has swept away the gatekeepers, the traditional media. In theory, the public sphere is now a completely open social space for the market of ideas. But hegemonic power is exerted by the mass media and the surviving geopolitical hegemon, the US. There is an imperative for governance, which must be written down in legal form. But laws or regulation may be obsolete before their ink dries, and the speed of their re-elaboration is no match for their targets; their bite is completely inadequate in a business environment that rewards violation of rights by design. A recourse to courts can sometimes be an effective option; but new, trustworthy gatekeepers are sorely lacking.

The second speaker spoke on a recent French experiment to regulate a social media platform like Facebook and some of its conclusions. First, common terms like "internet" or even "regulation" are too imprecise and not legally defined, and distinctions of country of origin and destination have little meaning anymore. Better to start by examining liability, in kind (criminal or not) and sequence (ex-ante or ex-post). The traditional model of legally enforced transparency with editorial responsibility, under decentralized supervision by peers and academia and animated by policy dialogue, is completely inadequate to deal with social networks. They exert little to no editorial function, even on the most egregious content, and display little genuine appetite for the responsibility.

"The era of self-regulation is over. Because it was based on trust, and trust is gone."

Attempts to spread false or malicious information is nothing new, but the potent vectors these platforms embody are. They and their outputs are not transparent by design, and they wield power not only by selection, but also by ordering and targeting information for their users. Their incentives have been until now quasi-exclusively to maximise traffic, harvest data, and monetise it; they need their attention focused on the side-effects of their actions. Enforcing more transparency would be a good start, but it needs to be done quickly; the authority and qualification requirements make however identifying who could do so problematic.

Participants painted a grim picture in the discussion. Process transparency won't help when the scale and precision of targeting is so vast, and malicious actors will evidently not disclose themselves. The root of the problem is the business model of data extraction and exploitation under the guise of free services. "Surveillance capitalism" has enabled profiling and targeting at a terrifyingly granular degree. Whether it fulfils its aims or not, its harmful effects are already being felt, to different degrees and impacts, across the world. "Communist" China is by no means spared. It is a model that involves three parties (user, data mining and processing company, and a corporate/government ecosystem that values and exchanges it), but that seems entirely unidirectional in its functioning, serving only actors who have the means to propagate information for their own purposes. Scientific campaigning has been twisted into subversive campaigning; the ground beneath governance and political science has shifted fundamentally.

"For corporations so large to have that much data, on so many citizens of the world… I have already seen small towns in England, that live from one globalised factory, led to vote for Brexit. It is a nuclear reactor and it needs to be shut down."

One participant questioned the demise of the country of origin/destination distinction. The speaker answered that purported fixes like more exemptions to the rules, or a reversal of the distinction in certain cases, would only risk further splinter markets, with potentially dangerous crashes. There should be unified regulation at a mass critical enough to establish its standard, with local enforcement within. Then governance can turn to the twin tasks of ensuring regulatory harmony within, and preventing interference from without. In the meantime however, it is far from clear what steps to change the system will have what effects, nor how to begin.

There was agreement on the need for more transparency and access to private data for research and regulatory purposes; it can be valuable to root out biases and distortions, intentional or not. One participant remarked that input and output transparency can be distinguished; in policy, this would translate to a need for ex-ante disclosure and ex-post review institutions, for full algorithmic accountability. Unlike many areas in the traditional economy that had institutions built up and needed deregulation, the digital world has evolved fast in a sparse institutional environment. It now needs more, and stronger institutions, to which authority to enact governance can be legitimately delegated.

Wrap-up – Lessons for global governance

In introducing the wrap-up session, the seminar organisers offered a few remarks on lessons learned from digital issues and their wider significance for the transformation of global governance. It was suggested that digital governance does display at least elements of "internet exceptionalism". Digital transformation has had massive impacts across economy and society, and across policy fields that require international coordination. It comprises a spectrum of topics ranging from technical questions of material infrastructure to elusive and volatile phenomena like behavioural manipulation. It is moving against global governance currents however: whereas the trend is to a shift from hierarchies tending to a multilateral ideal to a more networked, multi-stakeholder architecture, the demand here is mounting to develop stronger governance institutions to deal with issues linked to digital.

The multiplicity of these issues is impressive. They are profoundly reshaping the political economy, disrupting classical models of competition policy and regulation. They call territoriality in question, but do not abolish it; the "cyber-condominium" is an apt metaphor for the governance field of mixed private (national) spaces and commons. Normative decisions enshrined in human rights laws and judgements (privacy, transparency) can be powerful drivers for more and better regulation. The state of fragmentation of digital governance is, like in other governance fields but perhaps more so, a function of divergent preferences. Different normative orders create clashing jurisdictions; more so because of the intermediary and deterritorialised nature of issues touched by digital transformation. It

should be possible to find underlying principles to base minimal rules on, but how to ensure they have "bite" is unclear.

Underlying issues of governance in any policy field are two basic questions: *what* the issues actually are, and *who* has authority to deal with them, in a world where interdependence erodes sovereignty and governance actors are no longer exclusively public institutions. The discussion around digital governance seems to focus more on sifting apart the issues than defining responsibility; and acceleration seems to make any model obsolete before it can prove sustainable efficacy.

"Bias exists in society, and therefore machine learning will reflect this to some degree. But technology and the networks it enables can be powerful amplifiers of this bias."

In the ensuing discussion, one participant suggested that pressing for enforced accountability would at least begin to institutionalise the *who*, and recalled that while the problem of eroded territoriality in sovereignty is preoccupying, it should not draw attention away from equally pressing questions of redistribution. Others focused in China and remarked that its practice of digital governance has evolved from crude hardware control to sophisticated content control, moving rapidly to comprehensive data control. The recently created Cyberspace Administration of China has been elevated, answering to a leading group chaired by Xi Jinping. In line with its discourse on participating more proactively in global governance, China has moved on from seeing digital space as a matter for domestic control, no matter how tight. It asserts its model and interests in technical, policy and political international institutions (ITU, WTO, G20), and in bilateral relations with other states (pressures to choose Huawei for 5G, trade threats), building on its BRI initiative. In digital space, China split off early to create an extremely controlled (and repressive) ecosystem; but now, it is liberal-democratic governments that are in turmoil due to unchecked waves of content, malicious or not, that spread across their networks.

Programme

Friday 12 April 2019

13.30-14.00 Welcome and Introduction

14.00-15.15 **Session I - Digital governance in the broader global governance framework**. This first session will position digital governance challenges within the broader global governance framework, by examining actors involved, institutions in place, and the role of business, epistemic communities, NGOs and civil society in shaping the governance agenda. The session will focus on how the digital governance landscape has evolved and the main changes from a governance perspective.

15.15-16.30 **Session II - Internet infrastructure and national security**. With big data and transnational data flows, cybersecurity has emerged as a major business and policy concern with an obvious global governance dimension. In an environment where the decentralized internet architecture can be a cause of vulnerability and a loss of power for certain countries, this session will examine security in global networks and the governance solutions sought at the international level.

16.30-16.45 Coffee Break

16.45-18.00 **Session III - New competition concerns**. Digitalization has led to the concentration of data and information power in the hands of a few private actors and to competition concerns due to the "winner-takes-all" nature of big tech. This concentration also raises societal concerns related to the dissemination of disinformation and the responsibility of digital intermediaries. This session will examine the governance implications of an environment where data is concentrated in the hands of few actors and the regimes to regulate digital platforms and big tech.

19.30 Dinner and **keynote address**

Saturday 13 April 2019

09.30-10.45 **Session IV - Privacy and law enforcement issues.** Privacy concerns have accompanied the development of the internet but have taken on a new urgency when personal data, metadata and communication data are held in a jurisdiction which is different from the country in which they have originated. This has led to concerns related to the capacity of countries to enforce privacy laws abroad and access data for investigation. The session examines the implications of initiatives such as the GDPR and the Cloud Act.

10.45-11.15 Coffee Break

11.15-12.30 **Session V – Information control.** The global reach and ubiquitous use of the internet has made it into a potent tool for political communication, while also leading to calls for regulation of the content provided on websites and social media. The session will examine the governance challenges posed by hate speech, fake news, and international advocacy in the internet era.

12.30-13.00 **Wrap-up** - Lessons for global governance

- **Participants**

Caroline Atkinson	Peterson Institute for International Economics, USA
Michail Bletsas	MIT Media Lab, USA
Adrien Bradley	RSCAS, EUI, Italy
Joanna Bryson	University of Bath, UK
Luciana Cingolari	Hertie School, Germany
Madeleine de Cock Buning	STG, EUI, Italy
Jessica Dheere	Ranking Digital Rights, New America, USA
Paul Fehlinger	Internet & Jurisdiction Policy Network, France
Lisa Felton	Vodaphone, UK
Henry Gao	Singapore Management University, Singapore
Anita Gohdes	Hertie School, Germany
Eileen Fuchs	Federal Ministry of the Interior, Germany
Gerhard Hammerschmid	Hertie School, Germany
Elonnai Hickok	The Centre for Internet and Society, India
Philip Howard	Oxford Internet Institute, UK
Kristina Irion	University of Amsterdam, The Netherlands
Meelis Kitsing	Foresight Centre and Estonian Business School, Estonia
Christopher Kuner	Brussels Privacy Hub and VUB Brussel, Belgium
Paul Leonhardt	Federal Foreign Office, Germany
Judith Lichtenberg	Global Network Initiative, The Netherlands
Bruno Liebhaberg	Centre on Regulation in Europe, Belgium
Benoît Loutrel	Social Media Regulation Task Force, France
Chris Marsden	University of Sussex, UK
Milton Mueller	Georgia Institute of Technology, US
Manuel Muniz	IE School of Global and Public Affairs, Spain
Christopher Painter	Global Commission on the Stability of Cyberspace, UN
George Papaconstantinou	STG, EUI, Italy
Adam Peake	Internet Corporation for Assigned Names and Numbers, Belgium
Jean Pisani-Ferry	RSCAS, EUI, Italy
Andrea Römmele	Hertie School, Germany
Michel Servoz	European Commission, Belgium
Daniela Stockmann	Hertie School, Germany
Fabrizio Tassinari	STG, EUI, Italy
Rebekah Tromble	George Washington University, USA
Henri Verdier	French Ambassador for Digital Affairs, France

Yoshiaki Wada	NTT Data Corporation, Japan
Andrew Wyckoff	OECD, France