EVENT SUMMARY

INTERNET GOVERNANCE
International Legal Challenges

All-day Conference
Geneva, 27 November 2015

CONFÉRENCE DE LA SOCIÉTÉ SUISSE DE DROIT INTERNATIONAL

VENDREDI 27 NOVEMBRE 2015
Université de Genève, Uni Mail
Aula S130

INTERNET GOVERNANCE – INTERNATIONAL LEGAL CHALLENGES

Chaired by Prof. Dr. Christine Kaddous (Geneva)
and Prof. Dr. Rolf H. Weber (Zurich)

For more information please visit:
www.svir-ssdi.ch

Schweizerische Vereinigung für Internationales Recht
Société suisse de droit international

Geneva Internet Platform

Universität Zürich

FACULTÉ DE DROIT

UNIVERSITÉ DE GENÈVE

On 27 November 2015, the Swiss Society for International Law held an all-day conference exploring the international legal chalenges of Internet governance (IG). The event was organised and chaired by **Prof. Dr Christine Kaddous**, President of the Swiss Society for International Law (Faculty of Law at the University of Geneva) and **Prof. Dr Rolf H. Weber** of the (University of Zurich). The partner organisations included the Geneva Internet Platform (GIP)↗, the University of Zurich↗ and the University of Geneva↗. The conference brought together professors and IG experts from Lyon and across Switzerland to lead the discussion on this important and challenging topic.

Prof. Dr Alexandre Flückiger, Vice Dean of the Law Faculty (University of Geneva) and **Prof. Dr Christine Kaddous** inaugurated the conference to a full room of over 80 participants.

Prof. Dr Marco Sassòli launched the morning session with the following question: 'Internet is a supreme challenge to the Westphalian system. Without frontiers, how do [we] determine jurisdiction?'

The morning presentations aimed to tackle this question from three different perspectives: 1) Elements of a Legal Framework for Cyberspace, 2) Multistakeholder Participation in Cyberspace, and 3) Freedom of Expression in the Internet.

The afternoon session chaired by **Prof. Dr Daniel Girsberger,** delved deeper into specific legal frameworks on IG, examining 4) Privacy and Data Protection, 5) Jurisdiction in Cyberspace, 6) Alternative Dispute Resolution in Cyberspace, and 7) Cyber Security and Cyber Surveillance. Both sessions were followed by brief panel discussions.

The Conference was concluded by closing remarks of **Prof. Dr Rolf H. Weber**.

The following report summarises the key messages emerging from these conference presentations and panel discussions.

↗ Anytime you see this icon, there is more background material at http://digitalwatch.giplatform.org or other online resources.

1. ELEMENTS OF A LEGAL FRAMEWORK FOR CYBERSPACE

University of Zurich
Law Institute

Bridges for Future Foundations of Legal Framework

Complexity Matrix

Polycentric Regulation

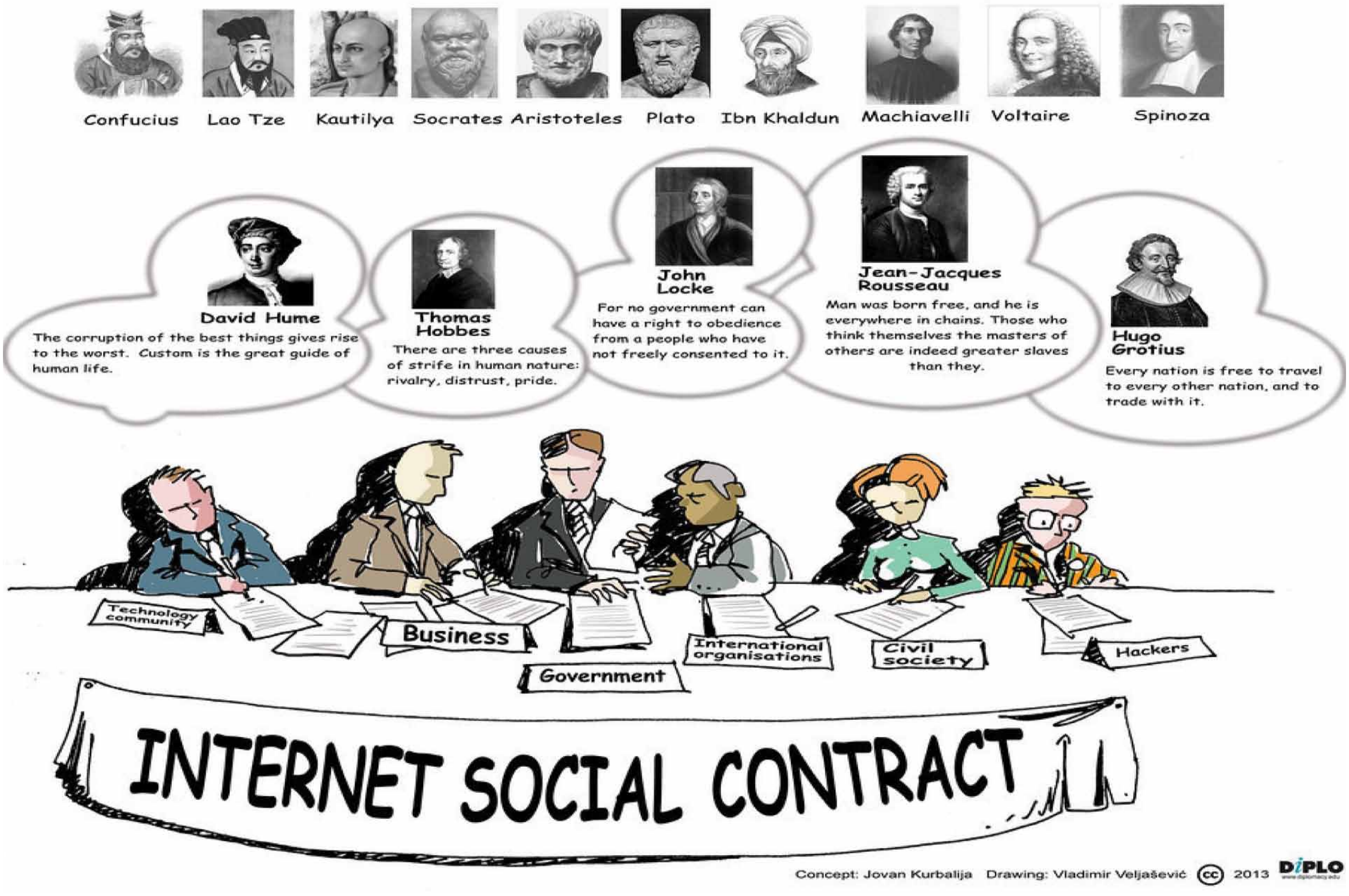
Hybrid and Mesh Regulation

Global Legal Pluralism

Global Experimental Governance

Prof. Dr Rolf H. Weber (Zurich) suggested that some lessons can be drawn from history to contribute to the elaboration of a legal framework for cyberspace, such as Rousseau's social contract theory. At the same time, new technologies are emerging faster than ever (e.g. Google's solar-powered Internet drones) and current legislative processes remain limited in their applicability to cyberspace.

Accordingly, Prof. Weber explored the *potential of soft law* (e.g. self-regulation) or customžary international law as possible alternatives. He also put forward some possible bridges for future forms of cyberspace governance, including polycentric regulation, hybrid and mesh regulation, and global experimental governance, the latter entailing an institutionalised and participatory transnational process. More substantially, he outlined some *key principles* that could guide a transnational cyberspace framework: *legitimacy* of the stakeholders involved, *quality* of regulatory strategies, *accountability* of Internet regulation, and technological *standardisation*. As we move towards establishing this cyberspace framework, Prof. Weber concluded that confidence will serve as its foundation.


Confucius
Lao Tze
Kautilya
Socrates
Aristoteles
Plato
Ibn Khaldun
Machiavelli
Voltaire
Spinoza
David Hume
The corruption of the best things gives rise to the worst. Custom is the great guide of human life.
Thomas Hobbes
There are three causes of strife in human nature: rivalry, distrust, pride.
John Locke
For no government can have a right to obedience from a people who have not freely consented to it.
Jean-Jacques Rousseau
Man was born free, and he is everywhere in chains. Those who think themselves the masters of others are indeed greater slaves than they.
Hugo Grotius
Every nation is free to travel to every other nation, and to trade with it.
Technology community
Business
Government
International organisations
Civil society
Hackers
INTERNET SOCIAL CONTRACT

Concept: Jovan Kurbalija Drawing: Vladimir Veljašević (cc) 2013 DiPLO

Visual Summary of an interplay between historical context and 'drafting' of the Internet social contract

2. MULTISTAKEHOLDER PARTICIPATION FOR CYBERSPACE

Prof. Dr Christine Kaufmann (Zurich) began by tracing the historical evolution of multistakeholderism as a concept, debunking the perception of multistakeholder initiatives as a new and recent phenomenon. In fact, multistakeholder forms of governance have existed through the twentieth century, beginning with the International Labour Organization's

(ILO's) tripartite structure established in 1919 and more recently the World Conference on Environment and Development held in Rio in 1992.

Multistakeholderism is defined by three main elements: the variety of actors involved (including non-state actors), an existing consensus on key principles and goals, and a participatory approach to decision-making. According to Prof. Kaufmann, multistakeholder initiatives have the potential to fill governance gaps if they are designed in a way to ensure *transparency, predictability, inclusiveness,* and *accountability* and are based on *consensus* about goals and procedures.

In the IG world, many models of multistakeholderism exist, such as the Internet Corporation for Assigned Names and Numbers (ICANN)↗, the World Wide Web Consortium (W3C)↗, and the Internet Society (ISOC)↗. While ICANN presents an example of a highly structured organisation, W3C and ISOC propose multistakeholder models that involve a less defined structure.

Conversely, *NETmundial*↗ was characterised by Prof. Kaufmann as 'multistakeholderism in its purest form'. What we conclude from this discussion is that there is no one-size-fits-all model for multistakeholder initiatives. Finally, Prof. Kaufmann echoed some of Prof. Weber's observations by underlining three key challenges in cyberspace multistakeholderism: ensuring legitimacy, ensuring transparency, and ensuring accountability. To address some of these challenges, expertise and lessons learned could be leveraged from the United Nations Guiding Principles on Business and Human Rights↗ and the National Action Plans that have been established to strengthen implementation.

3. FREEDOM OF EXPRESSION IN THE INTERNET

Prof. Dr. Maya Hertig (Geneva) discussed some of the challenges raised by the Internet in ensuring freedom of speech and expression↗. She underlined that *free speech principles* are essential within a democratic society and also contribute to societal progress through the sharing of ideas and production of research.

However, as other session speakers have also highlighted, new technologies have introduced new challenges to legal frameworks with regards to the Internet. On one hand, intermediaries (e.g. Google) make it much more difficult to identify the applicable jurisdiction.

On the other hand, legal frameworks must now adjust to the implications of *mass communication, mass surveillance* and issues surrounding *anonymity* and *censorship*. This generates a difficult balancing act between freedom of expression and privacy, *national security,* public order, dignity and other concerns. Likewise, it has become much more challenging to distinguish between public and private expression, and define what constitutes the "media" or "journalism.

Ultimately, Prof. Hertig anticipated that it will be a challenge to “design a clear, foreseeable legal framework for freedom of expression… a challenge we will still be grappling with in the future.”

The first panel discussion briefly examined territoriality and loss of sovereignty, US exceptionalism, legitimacy of multistakeholder processes, and the role of the UN Security Council in addressing radicalisation through the Internet.

4. PRIVACY AND DATA PROTECTION

Prof. Dr. Bertil Cottier (Lugano/Lausanne) recalled the evolution of data protection, with the Hippocratic Oath constituting the first privacy norm in history. *Sectorial privacy norms* have evolved to more *general data protection mechanisms,* including hard law instruments (e.g. 1981 CETS 108), soft law sources (e.g. 1980/2013 OECD Privacy Guidelines), and self-regulation texts and terms of service (e.g. Microsoft, Apple, Google, Amazon, Facebook).

The *terms of service* of these transnational companies in particular have an enormous impact compared to some of the soft law and self-regulation instruments. However, this diversity of instruments signals a ‘fragmented, outdated and uncertain legal framework’. Alongside the challenges of rapidly emerging technologies and complex communication channels, the legal framework on privacy remains precarious given the *paradoxical behaviour of Internet users:* Internet users tend to publicly share large quantities of private information while still demanding protection of their privacy.

In this context, Prof. Cottier noted: ‘We have to adapt to a new environment and new ways of regulating.’ Possible solutions include improving some of the existing mechanisms, unifying standards, and increasing soft law recommendations produced by international organisations.

Other possible avenues include more targeted interventions for service providers (e.g. regarding terms of service, guidelines on cloud computing), promotion of greater awareness among end users, or incorporating privacy directly within the design of new technologies.

COCA COLA METAPHOR

Prof. Cottier described metaphorically normative scale in digital policy in the range from regular Coca Cola (treaties and regulations) to Coca Cola Light (good practices). This metaphor was referred frequently in discussion on regulation of online human rights, jurisdiction and cybersecurity. For more information on normative scale you can visit http://www.giplatform.org/barometer

5. JURISDICTION IN CYBERSPACE

Prof. Dr Edouard Troppez (Lyon) began his presentation by asking: ‘Why is jurisdiction of cyberspace so complex?’ The answer is in the concept itself. In other words, *the myth of cyberspace* as a real place. Rather than using the term ‘cyberspace’, Prof. Treppoz recommended using the word ‘Internet’, as it is much more connected to the physical world and can be more clearly conceived of as a tool. Nevertheless, it remains difficult to determine the appropriate jurisdiction for Internet-related activities as the Internet is technically universal. This is especially challenging when examining *contracts* and *torts*. Contracts can involve the provision of intangible Internet-based services (e.g. music streaming) which frustrates the possibility of establishing jurisdiction based on the location of service delivery. Torts present similar questions on how to locate a cyber-tort.

Prof. Treppoz offers three possible approaches to tackling these challenges. First, jurisdiction can accept the universality of the Internet and hinge on the accessibility of the activity within the court’s territorial jurisdiction. Second, jurisdiction can consider the activity created by the Internet and try to localise this activity within country borders (e.g.

domain names, territorial scope of the right to be forgotten). However, Prof. Treppoz identified weaknesses with both of these approaches. Finally, the approach he favoured is to *circumvent the Internet* altogether and rather identify a connecting factor outside of the Internet that could be circumscribed within a national jurisdiction (e.g. the residence of the author of a website or the victim of the damages).

'Cyberspace does not exist' has been echoed in presentations by Prof. Troppez and Dr Kurbalija. The argument is that all elements of the Internet could be physically located: servers, cables, users, etc. Once they are physically located they are part of 'physical reality' and existing law can apply. One discussant argued that 'cyberspace' should be considered by lawyers and regulators as the new way through which users experience social interaction. This new experience shapes users' behaviour in a different way than 'physical reality'. Geographically speaking, cyberspace is not different from real 'space'. However, the social reality created by the Internet is different. Therefore the discussion on 'cyberspace' and law is likely to shift from geographical to social arguments. Further sociological and legal research is expected in this field.

6. ALTERNATIVE DISPUTE RESOLUTION IN CYBERSPACE

SVIR - SSDI / Geneva / November 27, 2015
Internet Governance – International Legal Challenges
Alternative Dispute Resolution in Cyberspace
Can ADR address the challenges of Massive Online Micro Justice?
Jacques de Werra
UNIVERSITÉ DE GENÈVE

Prof. Dr Jacques de Werra (Geneva) examined his coined concept of *Massive Online Micro Justice* (MOMJ) as a way of addressing the pressing need for developing alternative dispute resolution mechanisms on the Internet. Internet companies are increasingly under pressure from users to address their concerns. Since the European Court of Justice ruling on *the right to be forgotten* in May 2014, Google has received 345,846 requests for its implementation and 1,225,712 requests for removal of URLs. More broadly, can society rely on Google (or other Internet companies) as an adjudicator in Internet-related cases? Or should this be the function of entities with more public oversight? Accordingly, there have been calls for greater *transparency* in Google's adjudication process, to which Prof. de Werra added: 'Quantitative transparency is good; qualitative transparency is better, offering legal guidance to the platform is even better.'

A possible solution to address some of these concerns could be derived from an *alternative dispute resolution* (ADR) based on ICANN's Uniform Domain-Name Dispute-Resolution Policy (UDRP). The UDRP is based on global law and the decisions enforced are publicly available online. MOMJ Models could be structured so that challenged decisions made by platforms should be submitted to an independent and transparent ADR body with formalized procedural rules. This type of ADR could help to tackle the challenges of Massive Online Micro Justice and can promote *the right of access to justice for Internet-related disputes.*

7. CYBER SECURITY AND CYBER SURVEILLANCE

Dr Jovan Kurbalija, Director of DiploFoundation and head of the Geneva Internet Platform (GIP) concluded the conference presentations by clarifying some of the key issues directing discussions on cyberspace and cybersecurity.

First, he upheld Prof. Treppoz's point on 'Internet' as a more useful term to characterise cyberspace. Secondly, Dr. Kurbalija refuted the idea that cyberspace entails the end of sovereignty; in fact, governments have increased their ability to control cyberspace and cyber communications. Thirdly, he challenged the decentralised nature of the Internet showing that 90% of it flows through cables concentrated in 24 major centres worldwide. Finally, he emphasised *trust* as one of the underlying issues of cybersecurity discussions.

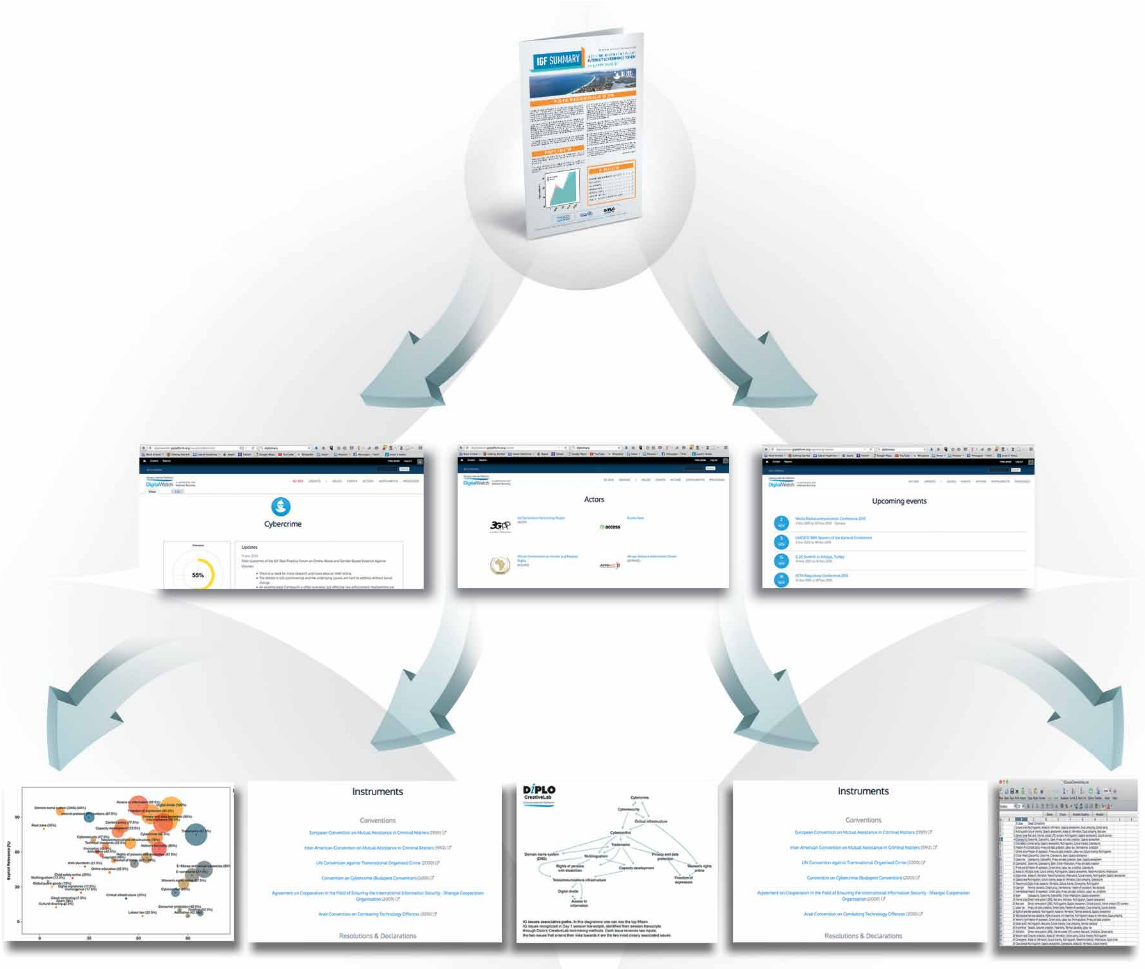
Dr Kurbalija then shifted the discussion to *the issue of terminology*. Using the text mining software developed for the *GIP Digital Watch*, Dr Kurbalija demonstrated the different terminologies for defining the Internet and how they have played a role in shaping IG discourse. In the context of cybersecurity, many inter-state discussions are centred on understand-

ing 'what are we are talking about': in the US/Euro-Atlantic approach, information security is understood as a subset of cybersecurity, while it is the opposite within the Chinese-Russian approach. Decisions on which terminology to use within cybersecurity discussions can therefore have important policy implications and can shift the focus of discussions to different IG issues.↗

Cybersecurity can also be divided into three areas for which numerous instruments exist: a) security *OF* the Internet (e.g. critical internet infrastructure↗); b) security *ON* the Internet (e.g. cybercrime↗, child safety online↗); and c) security *BY* the Internet (e.g. cyberterrorism). Cyber surveillance, on the other hand, relates to issues such as espionage, economic surveillance, privacy and data protection↗, and diplomatic immunities↗. Dr Kurbalija highlighted the emergence of international rules on prevention of the commercial use of data gathered by cyber surveillance. More information at these IG issues can be found on *GIP Digital Watch*↗.

Final panel discussions focused primarily on the concept of cyberspace, ICANN jurisdiction, and diplomatic immunities in the Internet era.

GIP DIGITAL WATCH REPORTING IN THREE LAYERS



On the **1st layer** you can find summary text and click on an icon ↗ that will lead you to...

...the **2nd layer,** where you can find more detailed information, including session reports, graphics, and information about the various actors. Click on the icon ↗ to go to...

...the **3rd layer,** where you can find primary sources, transcripts, legal instruments, raw data, and statistics

GIP Digital Watch is service provided by
Geneva Internet Platform

in partnership with
Internet Society

and members of the GIP Steering Committee
Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra
UNIVERSITÉ DE GENÈVE
DCAF
a centre for security, development and the rule of law
ETH BOARD

GIP Digital Watch is operated by
DiPLO
www.diplomacy.edu