

How to shape a successful digital ecosystem?

Polish-Swiss Innovation Day:

Warsaw, 23 May 2017

Keynote address by Dr Jovan Kurbalija



Dear colleagues,

It was a pleasure to meet you on 23 May for the Polish-Swiss Innovation Day. I enjoyed our discussion. It was great to learn about the impressive progress being made on the Polish digital scene.

What follows is my annotated presentation. You can also find indications on how to follow up on our session via online resources (Digital Watch Observatory), monthly briefings (11:00 UTC/13:00 CEST) on the last Tuesday of every month), and future meetings when you are in Geneva.

I am looking forward to (e) seeing you in Geneva, Warsaw, and online.

With best regards,

Jovan Kurbalija
Head, Geneva Internet Platform
Director, DiploFoundation



My keynote address outlined the policy challenges faced by digital start-ups. The practical focus was provided by following the life of an imaginary Internet company called Digita. Starting as an interesting theoretical idea, Digita developed into a real company facing many market, policy, and regulatory challenges. Using the example of Digita, I opened a discussion on how policy and regulatory frameworks can facilitate the innovation and growth of new digital companies.

What is Digita?

Digita is a start-up company established by a group of unemployed anthropologists and social scientists who met to discuss the problems they and other colleagues faced with finding employment. The idea for Digita emerged, following the Uber approach (platform economy). In the same way that Uber takes under-utilised cars out of garages and puts them into use, Digita takes expertise and knowledge from 'intellectual garages' and puts them to work addressing the growing demand for cultural tourism.

Geneva Internet Platform

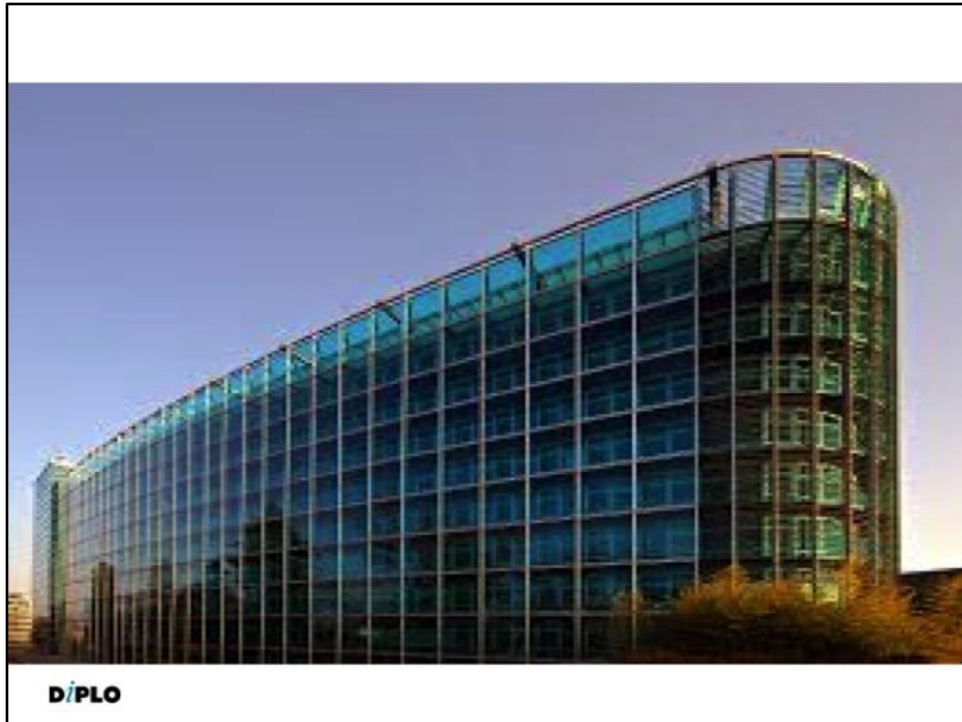


The Geneva Internet Platform is an initiative
of the Swiss authorities operated by DiploFoundation

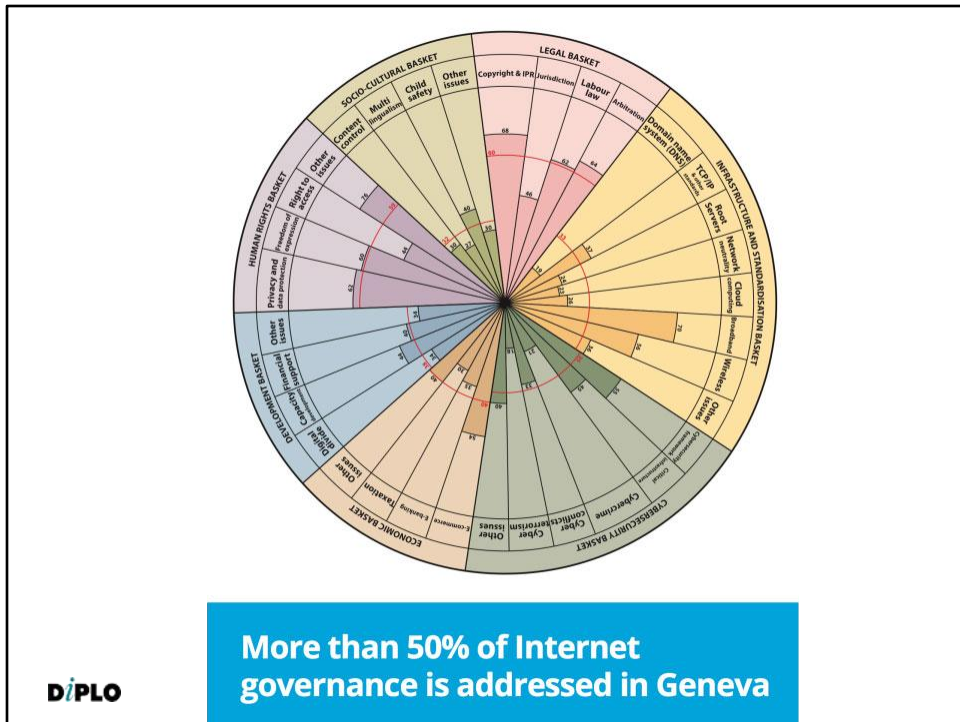


Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

***Di*PLO**
www.diplomacy.edu



DiploFoundation and the Geneva Internet Platform (GIP) are located on the second floor of the World Meteorological Organization (WMO) building, in the heart of International Geneva, 500 metres from the UN Palace and 100 metres from the World Trade Organization (WTO). You can join our activities and visit us for brainstorming and bilateral discussions on various aspects of digital policy.



According to a study conducted at the Geneva Internet Platform (GIP), more than 50% of Internet governance and digital policy issues are addressed in Geneva. The study provides an approximate indication of Geneva’s role in comparison with all other places globally. It is done by calculating the following indicators for each Internet governance issue:

WHO? Location: the number of Internet governance actors (e.g. international organisations, NGOs, think-tanks) based or represented in Geneva. The scoring of the indicator is as follows:

- 0 = No representation in Geneva
- 1 = Representation in Geneva
- 2 = Based in Geneva (official seat)
- 3 = Based in Geneva with less than 60% activities performed in Geneva
- 4 = Based in Geneva and all activities performed in Geneva

HOW? Decision-making: the number of legal and policy instruments adopted and managed from Geneva; the number of decision-making processes performed in Geneva (including approximate number of meetings and participants). The scoring of the indicator is as follows:

- 0 = No policy and legal instruments
- 1 = Occasional adoption of policy instruments (standards, recommendations)
- 2 = Regular adoption of policy instruments (at least three per year)
- 3 = Adoption of legally binding instruments
- 4 = Legally binding instruments with developed regime (secretariat, implementation, reporting).

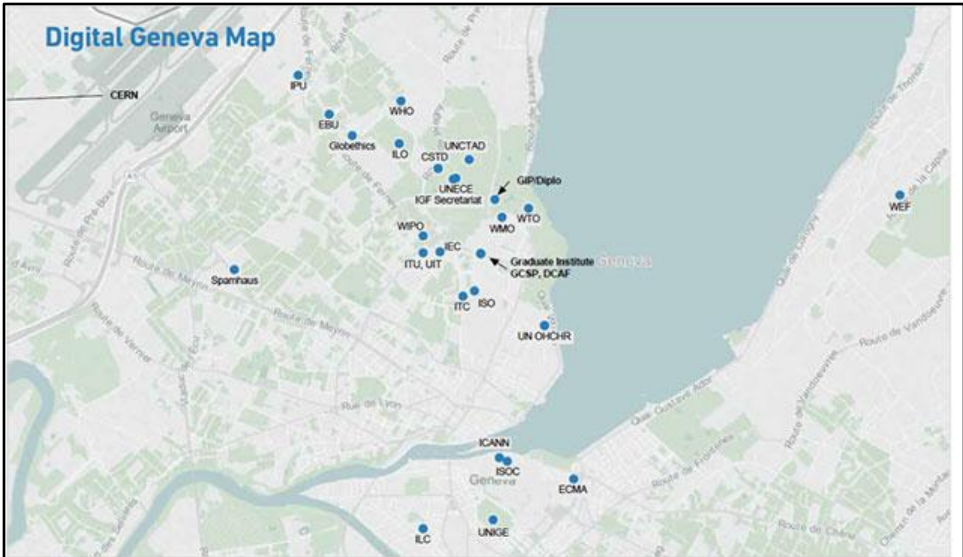
HOW? Decision-shaping: the number of events (conferences, panels, awareness-building sessions), research projects, and Internet spaces run by Geneva-based institutions (social media, Internet). The scoring of the indicator is as follows:

- 0 = No decision-shaping activities
- 1 = Occasional organisation of events
- 2 = Regular organisation of events (more than three per year)
- 3 = Preparing research and policy papers
- 4 = Comprehensive approach combining events, research, and prominent web presence

HOW? Relevance: The role of Geneva-based institutions and policy processes in addressing the most relevant Internet governance issues, including policy gaps and controversies. The policy study lists these issues in each issue area (e.g. infrastructure, legal issues, and development issues). The scoring of the indicator is as follows:

- 0 = No coverage of pressing Internet governance issues
- 1 = Decision-shaping coverage of relevant Internet governance issues (events, conferences, research)
- 2 = Policy-making coverage of relevant Internet governance issues
- 3 = Negotiation of legal instruments on relevant Internet governance issues
- 4 = Comprehensive coverage of relevant Internet governance issues (implementation, secretariat, reporting)

Digital Geneva Map



Geneva Actors

Commission on Science and Technology for Development
 Disarmament Foundation
 IAEA
 European Broadcasting Union
 European Organization for Nuclear Research
 Geneva Centre for Security Policy
 Geneva Centre for the Democratic Control of Armed Forces
 Graduate Institute of International and Development Studies
 ICJ for Peace Foundation

CSTD
 EBU
 ECR
 ECR
 ECR
 GICP
 GICP
 Graduate Institute
 ICAEW

International Labour Organization
 International Organization for Standardization
 International Documentary Centre
 International Electrotechnical Commission
 International Trade Centre
 Internet Society
 Office of the United Nations High Commissioner for Human Rights
 The International Centre for Democracy
 The Japanese Project
 United Nations Conference on Trade and Development

ILO
 ISO
 ITC
 ITC
 ITC
 ITC
 ITC
 ITC
 ITC

United Nations Economic Commission for Europe
 United Nations Human Rights Council
 United Nations Institute for Disarmament Research
 World Economic Forum
 World Health Organization
 World Intellectual Property Organization
 World Meteorological Organization
 World Trade Organization
 University of Geneva

UNICEF
 UNICEF
 UNICEF
 UNICEF
 UNICEF
 UNICEF
 UNICEF
 UNICEF



These two photos, from the inauguration of two popes, vividly illustrate the technological evolution. While technological change is obvious, there is an open discussion on the nature of these changes. Are they positive or negative? Is technology bad or good?

The short answer is that technology is neither good nor bad – nor is it neutral (Kranzberg's First Law). This statement is not as contradictory as it looks at first glance. Technology is not *inherently* bad or good. It can be used for bad or good purposes. Twitter has been used both for good causes (coordinating humanitarian assistance in Haiti) and bad causes (criminal gang communications).

While it is not *inherently* good or bad, it is not neutral either. Technology influences how we do things. It identifies new winners and losers. Every piece of technology empowers some individuals, groups, regions and/or countries. In the case of the Internet, it has empowered individuals (Zuckerberg – Facebook), groups (WikiLeaks hacker community), regions (e.g. Silicon Valley) and countries (Estonia and Malta, with their long-term e-development plans). Some incidental benefits have accrued through country code abbreviations, for countries such as Tuvalu – .tv and Montenegro – .me.



The Internet is an essential part of modern society. In particular, it is crucial for economic and societal development. For example, Internet access is often viewed as the 'invisible' sustainable development goal (SDG), horizontally influencing all the other SDGs.

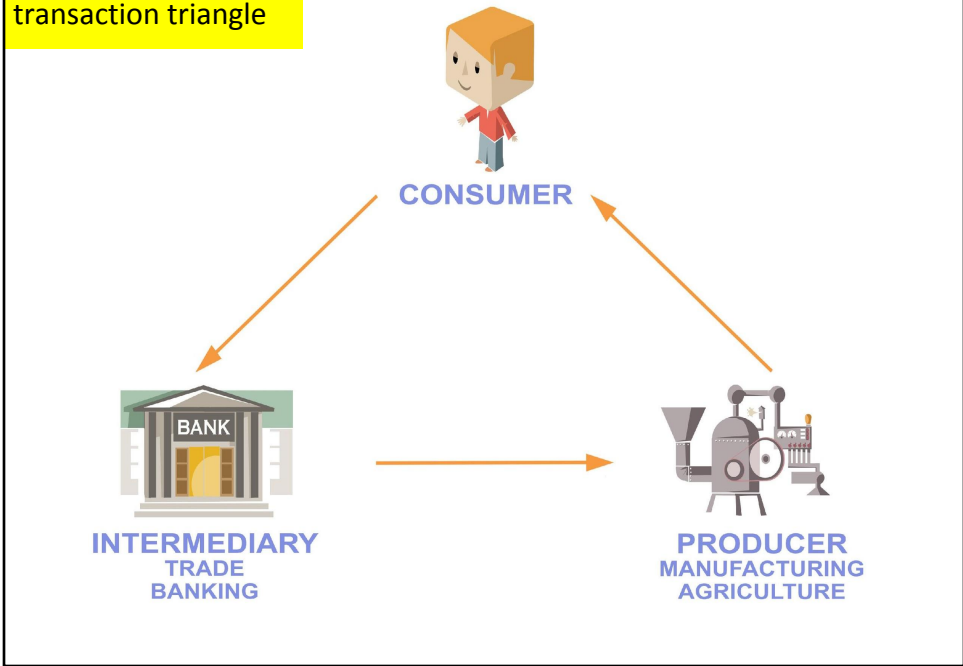
Flow of data and money on the Internet

In the next few slides we will visualise the flow of data and money on the Internet in order to see how the company *Digita* can develop its business model.

Geneva Internet Platform



Traditional economic transaction triangle



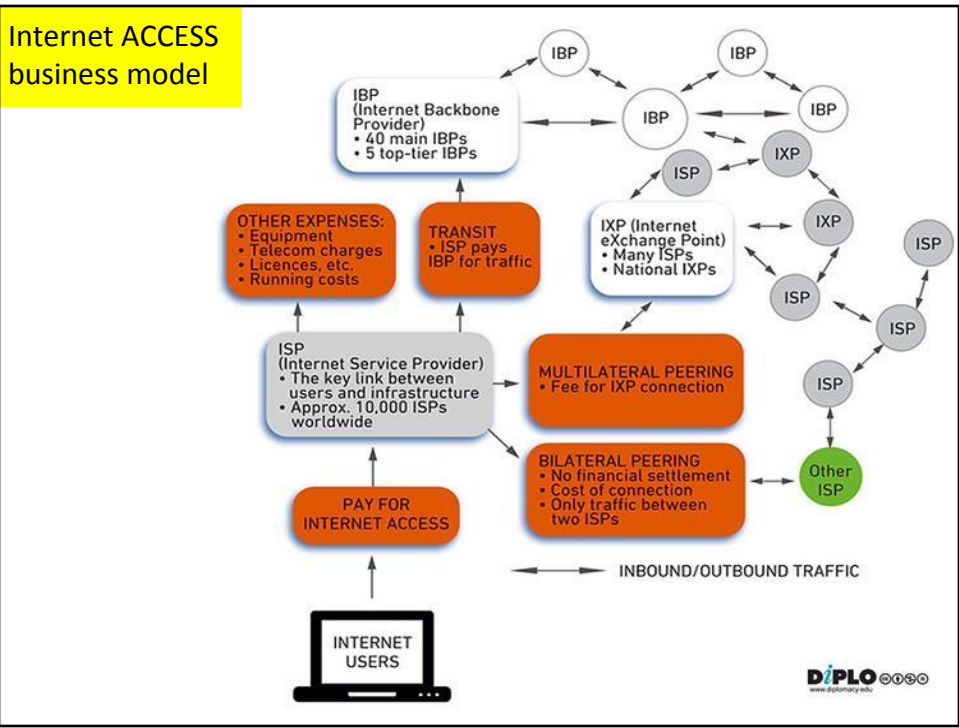
The traditional business model should be a reference point while discussing innovative business models on the Internet.

Hardware and software provider model



Selling hardware and software is one of the oldest business models in the digital field, existing before the Internet was invented. Today's main actors have evolved from IBM, one of the earliest providers of both hardware and software. Microsoft made perhaps the most important breakthrough by empowering personal computers with MS DOS and later the Microsoft Windows operating system. Likewise, Apple has been an important and long-time provider of hardware and software; even today, 68% of Apple's income comes from the sale of hardware and software. Lenovo and Samsung are also major providers of both hardware and software, and Cisco and Huawei are the most important providers of Internet networking hardware and software.

A recently emerged business model is the on-demand renting of software from cloud servers. For example, e-mail software on PCs is being complemented by Gmail. Word processor and spreadsheet applications such as Word and Excel are facing competition from applications such as Google Docs. Microsoft Office is now offered in the form of an annual subscription service instead of the once-off purchase of a software program. It is hard to place these new business models into neatly defined categories. Unlike the process of acquiring software – in which there is a clear money flow in the e-commerce transaction – the use of online software by individuals can be financially sustained by other means, such as the collection of data.



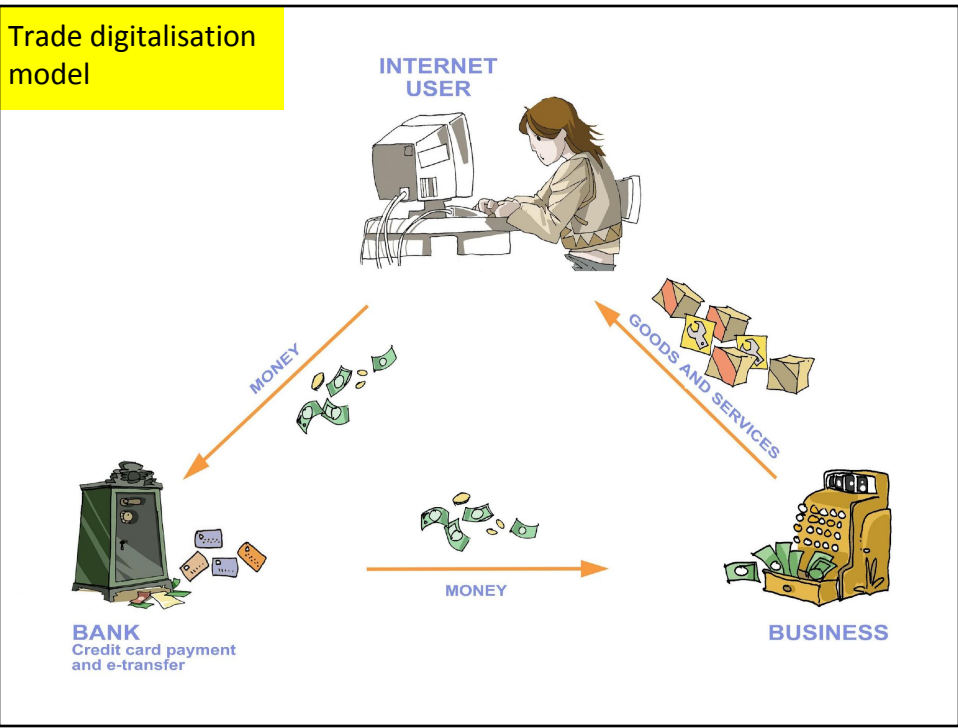
Internet users and companies pay Internet service providers (ISPs) for Internet-access-related services. Typically, ISPs use the fees collected to cover the following expenses:

- Cost of telecommunications expenses and Internet bandwidth to the next major Internet hub.
- Cost of IP addresses obtained from Regional Internet Registries (RIRs) or Local Internet registries (LIRs). Each device accessing the Internet needs an IP address.
- Cost of acquiring, installing, and maintaining equipment and software.

The Internet access business is becoming more complex due to governmental regulatory requirements in areas such as data-retention – for example, provisions that require telecommunication companies or ISPs to collect and store records documenting online activities. In some instances, more regulation leads to more expense, which is either passed to Internet users through subscription fees, or buffered by reduced profits for the ISPs.

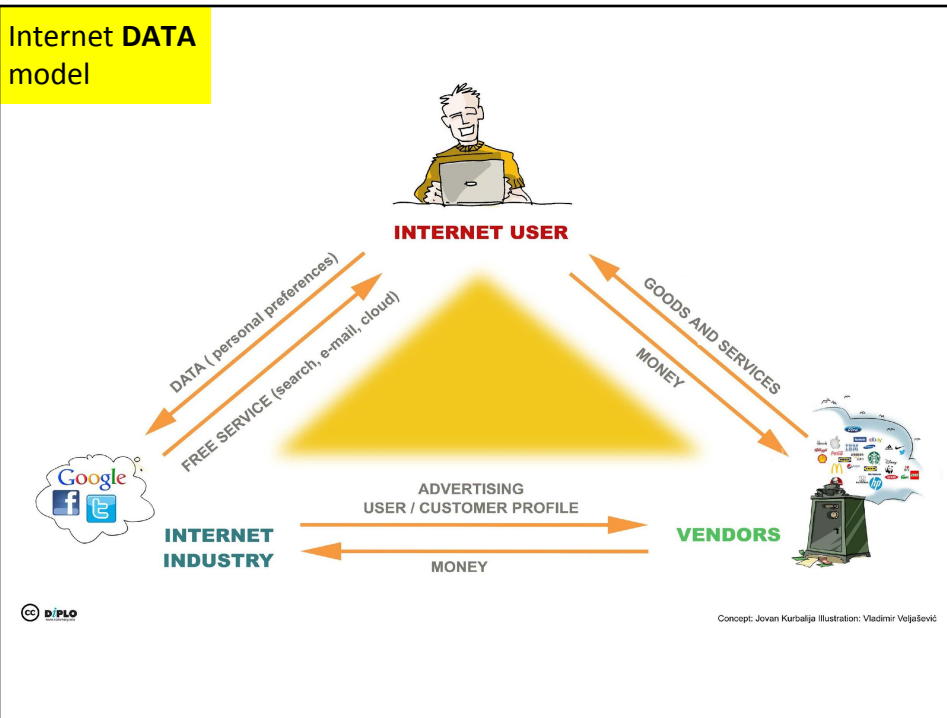
Telecommunications operators have raised the question of redistribution of the revenue generated by the Internet. They are trying to increase their share of the revenue pie generated by the Internet boom. So far, the main business beneficiaries of the Internet boom are Internet content companies. This is partly due to their innovative business model based on online advertising. Telecommunications companies argue that they should also benefit because *they* facilitate access to Internet content through *their* telecommunications infrastructure.

This discussion on the redistribution of Internet revenue strongly underpins the net neutrality debate – for example, should all Internet traffic be treated equally, or should it be segregated into different tiers, depending on the quality of services, payment, and reliability (e.g. a range of options from VIP Internet to an Internet for the poor)?



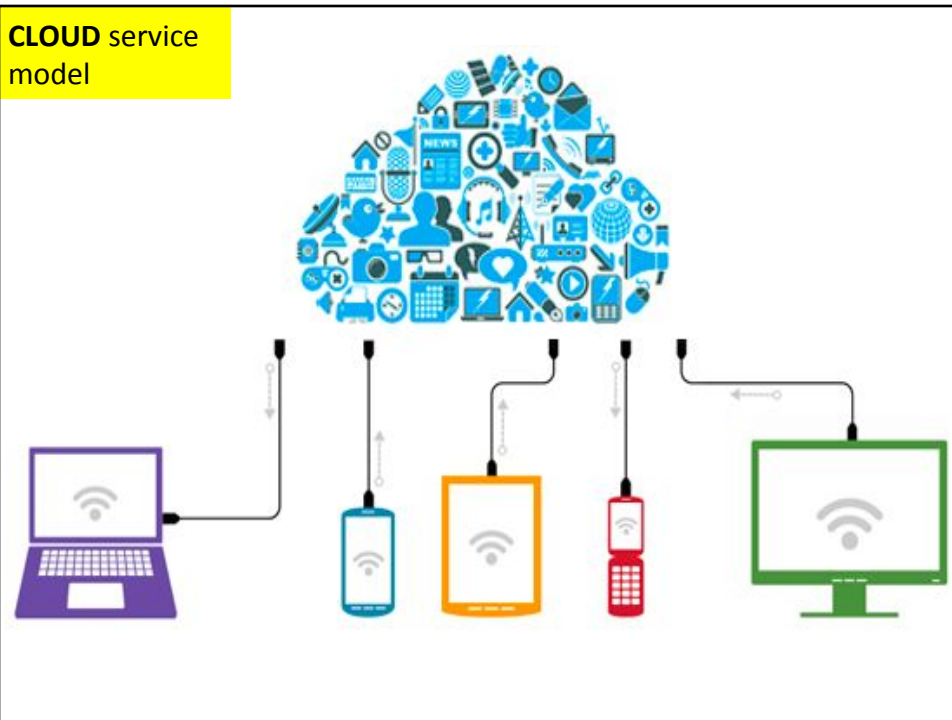
E-commerce started through the digitalisation of traditional bricks-and-mortar commercial transactions. It brought about numerous advantages for consumers, such as the convenience of online shopping, flexibility and easy access to different markets, and less time-consuming online banking and e-payment operations. E-bay, followed by Amazon, appeared as the main early player in e-commerce.

More recently, an advanced e-commerce model was utilised within the music industry. Companies like Spotify and Pandora have managed to develop a new revenue model, bringing life back into the profit-draining music industry, by providing access to the streaming of music for a recurring subscription.



The major business innovation starts with Internet data model. Data is essential for the successful growth of Internet companies such as Google and Facebook, which rely heavily on data-driven advertising for revenue. For example, 90% of Google’s revenue in 2015 (USD 75 billion) came from advertising (Rosenberg, 2016). Internet companies use data generated by users, such as behaviour and interests, in order to match the user to relevant vendors. Their effective use of data has also promoted the relevance of data from a peripheral business resource to a central one, sometimes described as the ‘oil of the digital economy’ (Srnicsek, 2016, p. 30). The centrality of data has extended to other industries as well as to the overall economy in many developed countries. For example, Uber uses traffic, driver, and passenger data to develop its offer structure and market positioning, while Rolls Royce is using the Internet to collect data for maintenance and further development of airplane engines. The new Internet business model does not charge users for the use of Internet services; rather, it generates income from selling information about users to advertisers, or in the words of Zysman and Kenney (2014) by ‘delivering its users to advertisers’.

In this new business model user data is the core economic resource. When searching for information and interacting on the Internet, users give away significant amounts of data, including personal data and the information they generate, i.e., their electronic footprint. Internet companies collect and analyse this data to extract bits of information about user preferences, tastes, and habits. They also mine the data to extract information about a group; for instance, the behaviour of teenagers in a particular city or region. Internet companies can predict with high certainty what a person with a certain profile is going to buy or do. In other instances, user data helps to improve the product itself, particularly in artificial intelligence (AI) applications such as computer vision and speech recognition.



Cloud computing can be understood as the shift from storing data on hard disks on our computers to storing data in servers within the cloud (i.e., big server farms). It offers ubiquitous access to data and services from any connected device around the world.

The first wave of cloud computing started with the use of online mail servers (Gmail, Yahoo!), social media applications (Facebook, Twitter), and online applications (Wikis, blogs, Google Docs).

Apart from everyday applications, cloud computing is extensively used for business software. More and more of our digital assets are moving from our hard disks to the cloud. The main players in cloud computing are Google, Microsoft, Apple, Amazon, and Facebook, who either already have developed, or plan to develop big server farms. Cloud-based e-commerce applications are also developing, allowing companies to respond quickly to market opportunities and challenges.

Cloud computing may pose jurisdiction issues, when, for example, content that is considered infringing by national authorities is hosted on servers located in a different country. National laws that require data localisation can engender similar difficulties. We will come back to jurisdiction issues in future modules of the course.

The centrality of data is explained by Zuboff (2016) in the following terms: 'once we understand this (centrality of data), it becomes clear that demanding privacy from surveillance capitalists or lobbying for an end to commercial surveillance on the Internet is like asking Henry Ford to make each Model T by hand'.

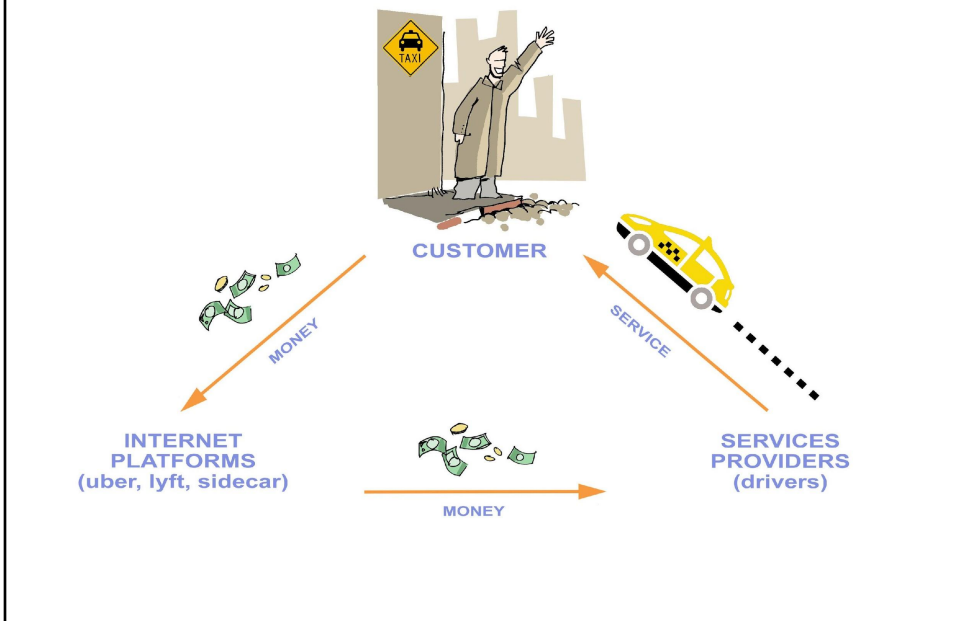
The fight for data is the fight for money. Internet and other businesses are in a 'gold rush' for data, which will determine their competitiveness and market survival. For example, telecommunication companies (Verizon, AT&T, Sprint) would like to tap into the data of their subscribers in order to sell it to advertisers. They try to copy data-driven models used by Internet companies such as Google and Facebook. In the United States, new regulations by the Federal Communication Commission (FCC) will allow telecommunication companies to use customer data for business purposes (Digital Watch, 2017). Even hardware companies are collecting data. Recent Wikileaks revelations showing that TV could be used for spying on users is not new: back in 2013, LG was investigated for using its Smart TV to get data about its users (Kelion, 2013).

At the same time, data-driven business models are facing risks and obstacles, including:

- Ad-blocking, which prevents Internet companies from advertising on participating platforms. The ad-blocking industry grew by 41% in 2015.
- New data-management software that provides users with more control of their data.
- New data protection and privacy policies affecting the industry's freedom to use data.

Limited possibilities to use data may affect business models. As Hal Varian (2015) from Google indicated, if companies cannot get enough revenue via data, they may move towards a pay-per-view mode. For example, Google may introduce micro-payments per search or resort to other payment options, such as subscriptions and fees, to compensate for reduced income from data.

Internet PLATFORM model



In an economic sense, a platform is the entity that allows or facilitates interaction between two sides in a market (OECD, 2011). Internet platforms facilitate economically driven interaction by using digital infrastructure and generate revenue from their intermediary roles (Srniczek, 2016). Internet platforms are the digital successor to pre-digital platforms, such as village markets or shopping malls.

Typically, the Internet platform model is based on the utilisation of resources which were not previously offered by the market. For example, Uber enabled privately-owned cars to be used similarly to taxis, and Airbnb allowed privately-owned rooms to be used analogously to hotel rooms. This business model has become attractive because it provides cheaper services and better user experience. For example, Uber tends to provide cheaper travel and facilitates smoother interaction with users by giving them the option not to pay with cash at the end of a ride, for example.

In an economic sense, a platform is the entity that allows or facilitates interaction between two sides in a market (OECD, 2011). Internet platforms facilitate economically driven interaction by using digital infrastructure and generate revenue from their intermediary roles (Srniczek, 2016). Internet platforms are the digital successor to pre-digital platforms, such as village markets or shopping malls.

Typically, the Internet platform model is based on the utilisation of resources which were not previously offered by the market. For example, Uber enabled privately owned cars to be used similarly to taxis, and Airbnb allowed privately owned rooms to be used analogously to hotel rooms. This business model has become attractive because it provides cheaper services and

better user experience. For example, Uber tends to provide cheaper travel and facilitates smoother interaction with users by giving them the option not to pay with cash at the end of a ride, for example.



For further reading on digital business models and the overall digital economy, consult the World Bank's *World Development Report 2016: Digital Dividends*. It is one of the most balanced and substantive studies available on both the opportunities and the risks of digital economic development. The title 'digital dividends' refers to benefits that digital technology delivers to society. The World Bank report shows that these benefits are not as significant as sometimes reported in 'optimistic studies'. The potential of digital development is high, but not yet realised by societies worldwide.

Policy Challenges for *DIGITA*

Digital Trade Rules
Privacy and Data Protection
Cybersecurity
Jurisdiction
Virtual Currencies

Geneva Internet Platform

The logo for the Geneva Internet Platform, which consists of a blue, horizontal, brush-stroke-like shape.

Policy Challenges

DIGITAL TRADE RULES

Geneva Internet Platform



In practice, trade barriers can be eliminated unilaterally, on a reciprocal basis through regional trade agreements (RTAs), or at a multilateral level. International agreements are needed through which governments bind themselves to a contractually defined (and thus transparent and foreseeable) behaviour.

International trade policies that aim to set out the applicable rights and obligations are called policies of *integration*. We can distinguish the following levels of integration:

- *Bilateral commercial (sectoral or comprehensive) agreement*
- *Free trade area* (e.g. EFTA, CEFTA, NAFTA, Association Agreements with the EU) which stipulates among the partners the elimination of all tariffs and quantitative restrictions on essentially all trade, but does *not* provide for common external trade policies. Market access rules remain sovereign
- *Customs union* (e.g. MERCOSUR), which eliminates customs within the area, *and* has a common external trade policy. Market access rules remain sovereign
- *Single market* (e.g. European Economic Area – EEA), which is a customs union *plus* common internal market (access to market) legislation. The goal is that the movement of capital, labour, goods, and services between the members is as easy as within them
- *Economic and monetary union* (e.g. the EU)
- *Comprehensive multilateral trade agreements* (e.g. WTO agreements)

The overall aim of all these agreements is to level the playing field for national and foreign economic operators, thus allowing for fair competition. These agreements are underpinned by two key principles: most-favoured-nation (MFN) and national treatment (NT). The MFN principle prevents WTO members from discriminating between their trading partners. If a country decides to grant a special advantage or favour to one of its trading partners (such as a lower customs duty rate for one of their products), it will need to extend that privilege 'immediately and unconditionally' to all other WTO members (GATT, Art. I).

The NT principle establishes that WTO members have to provide foreign products in their territory 'no less favourable' treatment than that accorded to like domestic products. This applies in respect of all laws, regulations, and requirements affecting their internal sale, offering for sale, purchase, transportation, distribution, or use (GATT, Art. III).



As the key policy player in modern global trade, the WTO has established a system of agreements regulating international trade:

- the [General Agreement on Tariffs and Trade \(GATT\)](#), dealing with the trade in goods;
- the [General Agreement on Trade in Services \(GATS\)](#) and its Annex on [telecommunications services](#);
- the [Telecommunications Services reference paper](#);
- the [Understanding on Commitments in Financial Services](#);
- and the [Agreement on Trade-related Aspects of Intellectual Property Rights \(TRIPS\)](#).
- In addition, the [Information Technology Agreement \(ITA\)](#) also touches upon digital-related aspects.

Within this framework, the WTO regulates many relevant digital commerce issues, including telecommunications liberalisation, intellectual property rights (IPR), and some aspects of ICT development. Digital commerce has a role in the following WTO activities and initiatives:

- A temporary moratorium on custom duties on electronic transmissions, introduced in 1998, renders all e-transmissions free of custom duties among WTO member states.
- The WTO [Work Programme on Electronic Commerce](#), established in 1998, sets out responsibilities for WTO bodies in e-commerce related areas.
- A dispute resolution mechanism which addresses, among others, cases involving electronic transactions, if they are covered under any of the existing WTO

- agreements. (One example is the [USA/Antigua and Barbuda Online Gambling](#) case, where e-commerce was particularly relevant.)

The Work Programme on Electronic Commerce established a broad definition of e-commerce, which 'is understood to mean the production, distribution, marketing, sale or delivery of goods and services by electronic means' (WTO, 1998a). This means that e-commerce encompasses various degrees of digitisation. A transaction may be considered e-commerce even if some part of it is not done digitally.

The Work Programme on Electronic Commerce also instructed four councils of the WTO to examine and report on the treatment of this issue:

1. The **Council for Trade in Services (GATS)** was tasked to examine and report on the treatment of electronic commerce in the GATS legal framework. One of the first points of discussion in the Council was the applicability of GATS to electronic commerce, which led to a reflection on the definition of trade in services. GATS defines trade in services as the supply of a service through any of four modes: cross border supply (mode 1), consumption abroad (mode 2), commercial presence (mode 3), and presence of natural persons (mode 4) (Article I:2). GATS takes an approach of 'technology neutrality', as it makes no distinction between the different technological means by which a service may be delivered and covers the supply of services through electronic means in the same way as all other types of delivery (WTO, 1998b). Moreover, electronic delivery can take place under any of the four modes of supply.
2. The **Council for Trade in Goods (GATT)** was tasked to examine and report on aspects of electronic commerce relevant to the provisions of GATT. The key issues proposed for analysis encompass topics related to market access; valuation issues; import licensing procedures; customs and other duties; standards in relation to electronic commerce; rules of origin; and classification.
3. The **Council for Trade-related Aspects of Intellectual Property Rights (TRIPS)** was tasked to examine and report on the intellectual property issues arising in connection with electronic commerce. The key issues proposed for analysis encompass topics such as protection and enforcement of copyright and related rights; protection and enforcement of trademarks; and new technologies and access to technology.
4. The **Committee on Trade and Development (CTD)** was tasked to examine and report on the development implications of electronic commerce, taking into account the economic, financial, and development needs of developing countries.

Policy Challenges

PRIVACY AND DATA PROTECTION

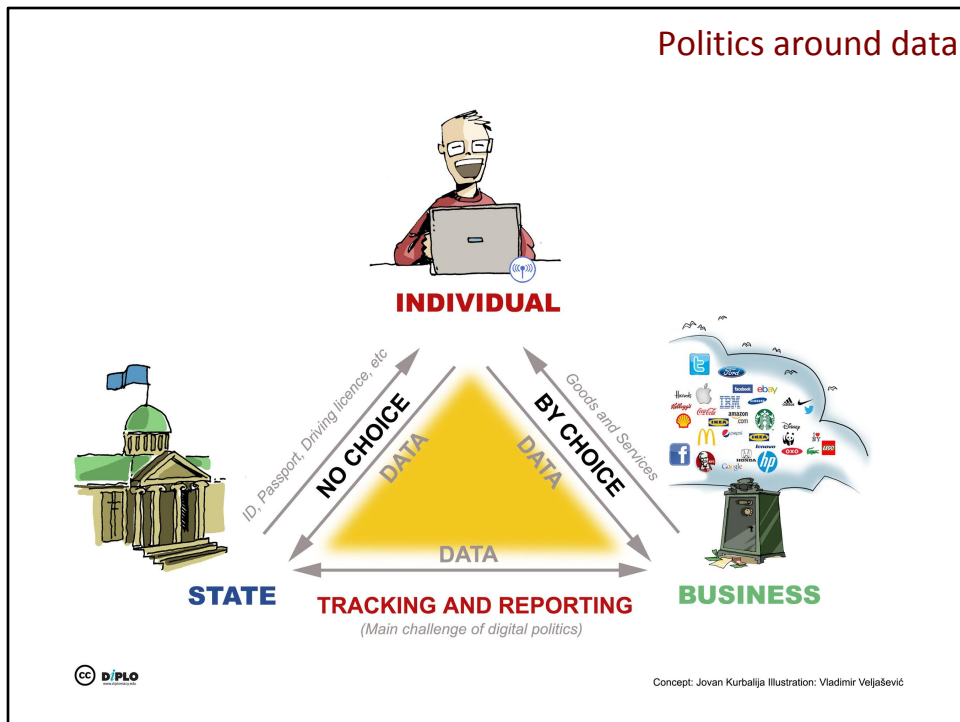
Geneva Internet Platform



Privacy and data protection frameworks can have a direct and profound impact on digital commerce. In particular, they can affect sectors that depend heavily on data, not only in the field of digital commerce, but also in the data-intensive Internet industry.

Standards for data exchange could also affect digital commerce. For example, data portability – the possibility of moving our data from, for example, one social network to another – directly impacts the Internet industry. Data presents a cross-sectoral impact that could be identified in other policy fields (competition rules, consumer protection, etc.).

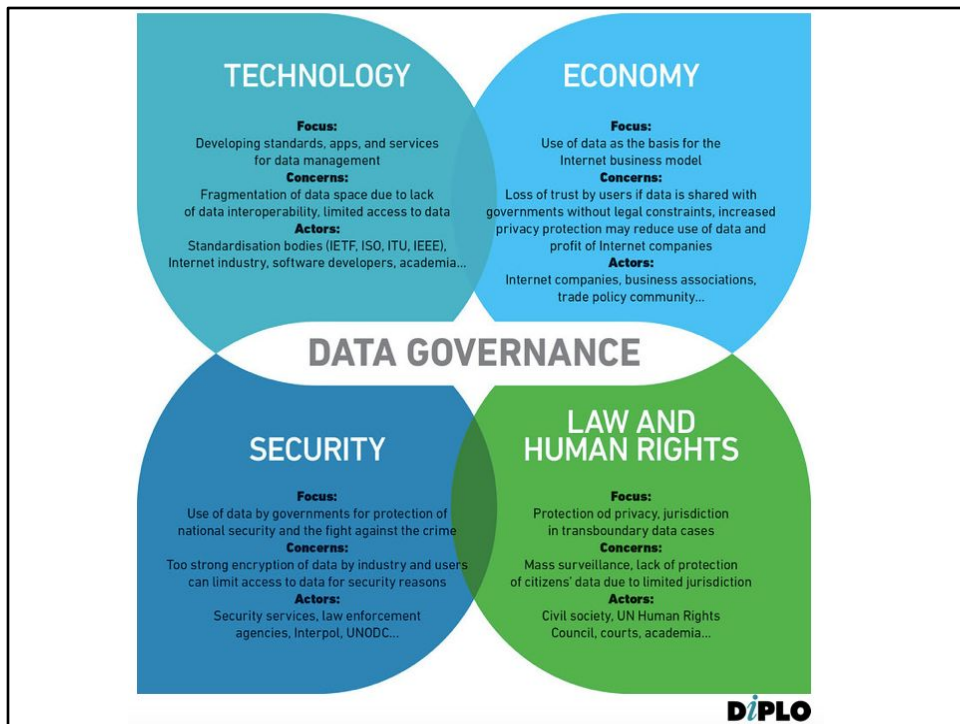
Privacy and data protection are two interrelated Internet governance issues. Privacy is usually defined as the right of citizens to control their own personal information and to decide whether or not to disclose it. Data protection is a legal mechanism that ensures privacy. Privacy is a fundamental human right. It is recognised in the Universal Declaration of Human Rights (UDHR), the International Covenant on Civil and Political Rights, and in many other international and regional human rights conventions.



The main privacy issues can be analysed using a triangle among individuals, states, and businesses. In this triangle, digital commerce is particularly affected by the trust of individual users in how businesses handle their data. The Internet industry has become more sensitive about strengthening user trust, in particular after the Snowden revelations. Trust is also affected by the unequal power of individual users and Internet companies. This is exemplified by the fact that Internet companies tend to change their privacy policies often, and do not give users a real choice besides the usual 'take it or leave it' approach, in which users can either accept the the new privacy policy or have the service suspended (Venturini *et al.*, 2016).

The third side of the privacy triangle is the least publicised, yet perhaps the most significant privacy issue. Both states and businesses collect considerable amounts of data about individuals. States put a lot of pressure on Internet business companies (e.g. Facebook, Google) to grant access to data to support their anti-terrorist and anti-criminal activities. As an example, after the Paris terrorist attacks in November 2015, the French government relied heavily on data provided by the Internet industry. Similarly, governments are increasingly concerned about stronger encryption used by the Internet industry, which makes the surveillance of Internet traffic more difficult.

The business sector is trying to resist governmental pressure and limit access by state authorities to their data. If government authorities gain access to business data, this can reduce the level of trust among Internet users and affect the business model of Internet companies. This tension between state authorities and the business sector will continue to be one of the underlying issues in global digital policy in the forthcoming period.



This graphic shows the policy interplay in data governance among four main areas: technology, economy, security, and law and human rights. It shows a summary of the main international instruments and regulations on privacy and data protection.

One of the main international instruments on privacy and data protection is the 1981 Council of Europe (CoE) Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, known as [Convention 108](#). Although it was adopted by a regional organisation, it is open for accession by non-European states. Since the Convention is technology neutral, it has withstood the test of time.

The EU has been one of the major promoters of privacy and data protection, affecting the global digital policy landscape in many respects. In this context, we will mention two examples with major potential impact on digital commerce: (a) the EU General Data Protection Regulation (GDPR); (b) the Privacy Shield between the USA and the EU. The EU adopted the GDPR in 2016 and it will become applicable from May 2018. Once in force, the EU regulation will affect the way private companies and organisations handle EU citizens' data.

The GDPR is intended to harmonise data protection laws in EU member states. It also gives EU citizens much more control over their data, for example, by allowing users to move data (portability), or to demand the erasure of their data (right to be forgotten). At the same time, it imposes strict and onerous obligations, requiring companies regardless of where they are based to adhere to compliance requirements and standards of security. For example,

companies must clearly ask for the data subject's consent for data processing; many companies will also be required to appoint a data protection officer (DPO).

One consequence is that the GDPR will have extraterritorial effect, as it will apply also to non-EU organisations that offer goods and services in the EU, or monitor the behaviour of data subjects within the EU. Non-EU companies will therefore have to see whether their activities fall within the scope of the regulation. A major challenge is that, in some cases, these companies will have to adopt a new mindset, especially if their practices and local data protection laws have not been as stringent as in the EU. If they do fall within its scope, they will be required to bring their practices in line with the strict data collection and handling practices, including the appointment of a DPO in certain cases, and the adoption of transparency measures.

The Privacy Shield addresses the sharing of data across the Atlantic Ocean – the major data highway in the world – between the EU and the USA. Whatever happens along this 'data highway' will affect digital commerce globally. The Privacy Shield is an attempt to reconcile differences in how the EU and the USA regulate data protection in cases in which data of EU citizens is hosted in the USA. A few questions have been raised: How can the EU ensure that data about its citizens is protected according to the rules specified in its data protection regulations? Do EU or US rules apply when handling data transferred through a company's network from the EU to the USA?

Initially, the EU and the USA solved this regulatory dichotomy via the Safe Harbour Framework that ensured that EU citizens' data was protected according to EU rules even if the data was located on servers based in the USA. The agreement allowed EU regulations to be applied to US companies inside a legal 'safe harbour'. US companies handling EU citizens' data could voluntarily sign up to observe the EU's privacy protection requirements.

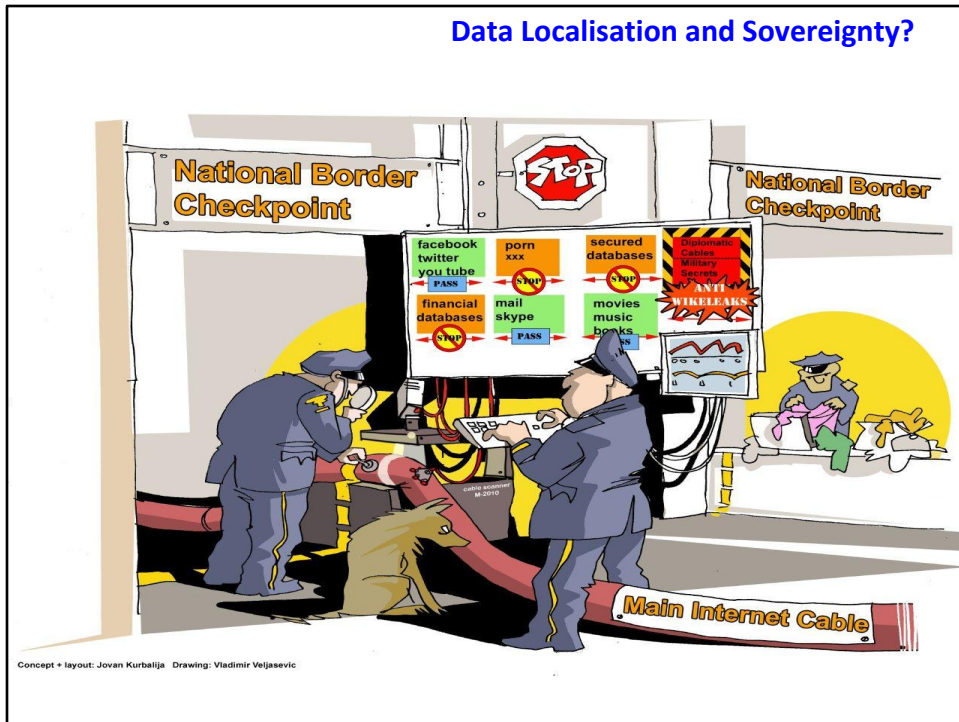
However, in October 2015, the European Court of Justice invalidated the Safe Harbour Framework on the grounds that the European Commission had not appropriately evaluated whether the USA maintains 'essentially equivalent' protection of EU citizens' data. This decision triggered negotiations between EU and US diplomats in search for a new mechanism. These negotiations resulted in the Privacy Shield, approved by EU member states in July 2016, with four countries abstaining – Austria, Bulgaria, Croatia, and Slovenia. Later that month, the European Commission formally adopted a decision confirming the adequacy of the EU-USA Privacy Shield.

The Shield imposes stronger obligations on US companies to protect EU citizens' personal data, and requires the US government to more robustly enforce the new provisions and monitor their implementation. In addition, the Privacy Shield also addresses one issue that has presented a major area of concern: the US government's access to the personal data of EU citizens. The Shield brought in written assurances from the USA that any such access would be subject to appropriate limitations, safeguards, and oversight mechanisms. The US government has also committed to cooperating with data protection authorities in the EU, as well as to creating an Ombudsperson mechanism for receiving and responding to

complaints from individuals regarding US government access to their personal data.

Another key international – but non-binding – document on privacy and data protection is the OECD Guidelines on Protection of Privacy and Transborder Flows of Personal Data from 1980, updated in 2013. These guidelines, and the OECD's subsequent work, have inspired many international, regional, and national regulations on privacy and data protection. Today, virtually all OECD countries have enacted privacy laws and empowered authorities to enforce those laws.

Data Localisation and Sovereignty?



Data localisation policies should be assessed against this changing economic scenario. Data localisation can be voluntary or forced. The first happens when a company decides to store its data on servers located in a particular jurisdiction for reasons that may vary from competitive advantages to better legal environment. The second is related to requirements made by national law.

Data localisation provisions can take different approaches, which pose different problems when it comes to their compatibility with trade norms. Some data localisation laws determine that companies should store data on servers located within the national territory and enforce limitations for data transfer and data processing; others ask companies to influence the routing of data packages (e.g. Deutsche Telekom's proposal to reroute data within Germany, or the seemingly now abandoned concept of a 'Schengen Cloud'). There are also proposals for mandatory local purchasing or local ownership of data storage equipment, limitations on foreign online retailers, and forced local hiring provisions.

In the wake of Edward Snowden's revelations, governments began to increasingly consider enacting data localisation norms which limit the storage, movement, and/or processing of digital data to specific geographies, jurisdictions, or companies. By keeping data stored within national jurisdictions, or by prohibiting data from crossing

‘untrustworthy’ territory or infrastructure, data would be better protected.

Those in favour of data localisation present it as a way to curb foreign surveillance, to protect citizens and businesses from threats to privacy, and to preserve national security. Critics of data localisation, however, see these measures as opportunistic protectionism that aims to use the Snowden backlash as an opportunity to develop domestic clouds and other technology services. Data localisation would lead to economic costs for the implementing economy, primarily through losses in productivity and competitiveness.

As concepts such as ‘data sovereignty’ and ‘data nationalism’ become more widespread in policy circles, data localisation gains traction worldwide and could become a non-tariff barrier to trade.

Bauer *et al.* (2014) developed and applied a method to calculate the economic impact of some enacted or proposed data localisation legislation on GDP in seven countries: Brazil (-0.2%), China (-1.1%), the EU (-0.4%), India (-0.1%), Indonesia (-0.5%), Korea (-0.4%), and Vietnam (-1.7%). Welfare losses (expressed as actual economic losses by the citizens) amount to up to USD 63 billion for China and USD 193 billion for the EU. For India, the loss per worker is equivalent to 11% of the average month salary; in China it is 13% and in Korea and Brazil, 20%.

Small and medium-sized enterprises (SMEs) can be particularly vulnerable to costs arising from domestic regulations, as they are less able to adjust their supply chains. Given their smaller scale, they must also distribute fixed costs resulting from regulations over a smaller volume of sales compared to larger firms.

Concerns over data localisation provisions range from technical to economic and human rights issues. By restricting data flows and competition between firms, localisation could increase costs for Internet users and businesses, could retard technological innovation, and could reduce the ability of firms to use cloud services and data analytics, for example. From a technical standpoint, restricted or forced routing leads to inefficient data traffic. Widespread adoption of data localisation could lead to the fragmentation of the global Internet and, with it, the fragmentation of global communication and commerce (Drake *et al.*, 2016).

Human rights advocates also point to potentially negative effects on freedom of expression and privacy, since some of the countries that adopted or are considering data localisation provisions do not have strong data protection frameworks in place to protect citizens from undue access to personal information by their governments and the private sector (Plaum, 2014).

The most emblematic example of a national data localisation law is the one adopted by Russia. The law, enacted in September 2015, mandates that data operators who collect personal data about Russian citizens ‘record, systematize, accumulate, store, amend, update and retrieve’ data using databases physically located in Russia (Morris, 2016). Roskomnadzor, the Russian agency responsible for enforcing the law, conducted a series of company inspections in order to assess compliance with the norm. The penalties for non-compliance vary from a formal warning to fines and the blocking of the company website or platform. In November 2016, LinkedIn, owned by Microsoft, was blocked after allegedly failing to comply with the data localisation provision. Until the present moment, LinkedIn and the Russian authorities have not managed to reach an agreement that would restore access to LinkedIn in the country.

Many other countries also adopted data localisation provisions (Drake *et al.*, 2016). For example, Australia prohibits the export of personally identifiable health records; Switzerland requires the prior consent of data subjects before financial records can be transferred across borders; some Canadian provinces require that some government institutions store personal data domestically; South Korea prohibits the storage of mapping data on servers outside the country. Vietnam also adopted a data localisation law in 2013, which makes it mandatory for every online service provider to keep a copy of all Vietnamese data on a local server, so national authorities can access it if needed. India is discussing data localisation measures, which are included in a paper about cloud services, issued by the Telecommunications Regulatory Authority.

The European Commission also presents a strong stance on the issue of data localisation, but it opposes these provisions. The free flow of data is considered a corollary of the four freedoms of the EU single market: free movement of goods, workers, service provision, and capital (European Commission, 2017). Nevertheless, the study *Facilitating cross border data flow in the Digital Single Market* revealed that several countries in the EU present data localisation provisions (Godel *et al.*, 2016). Location is seen by many market participants as a proxy for substantial assurances in terms of data access, privacy, audit, data integrity, and law enforcement. If existing data localising measures were removed, GDP gains are estimated at 8 billion euros per year (Bauer *et al.*, 2016).

Some European private actors also have strict ‘data residency’ requirements, not necessarily based on any formal legal restrictions. According to the European Commission (2017), unjustified restrictions on the free movement of data are likely to constrain the development of the EU data economy, therefore EU countries that

have data localisation provisions should revisit them. The new GDPR aims to provide additional reassurance to the free flow of data by guaranteeing that norms related to privacy and data protection will be applied uniformly in all EU member countries. The protection of privacy cannot be invoked as an argument to hinder the flow of data under the new GDPR.

The Commission recognises, nevertheless, that data localisation requirements may be justified and proportionate in particular contexts or in relation to certain data, especially before effective cross-border cooperation arrangements are put in place, such as ensuring the secure treatment of certain data pertaining to critical energy infrastructure, or the availability of electronic evidence for law enforcement authorities.

When it comes to EU relation with third parties, the Commission committed to try to include rules guaranteeing cross-border data flows in trade agreements elaborated between the EU and its partners, in order to curb new forms of 'digital protectionism' such as data localisation provisions (European Commission, 2017).

Data localisation was included in the Trans-Pacific Partnership (TPP), a trade agreement proposal between Australia, Brunei, Canada, Chile, Japan, Malaysia, Mexico, New Zealand, Peru, Singapore, the United States (until 23 January 2017), and Vietnam. A general provision forbade contracting parties to require the localisation of 'computing facilities in that Party's territory as a condition for conducting business in that territory'. The proposal, allows, however, the adoption of measures inconsistent with the data localisation prohibition, under some circumstances, to achieve a legitimate public policy objective.

Policy Challenges

CYBERSECURITY

Geneva Internet Platform





Cybersecurity is often mentioned as one of the preconditions for the rapid growth of e-commerce. Cybercrime is one of the main cybersecurity risks, with profound effects on digital commerce and the Internet as a whole. There are a number of estimates of the annual costs of cybercrime for the global economy. In 2014, the security company McAfee estimated the annual cost of cybercrime for the global economy at USD 445 billion (CSIS and McAfee, 2014). In 2015, the British insurance company Lloyd's estimated the costs for business at about USD 400 billion per year (Gandel, 2015). In its research, Juniper, a global vendor of Internet products, estimates that cybercrime will cost the business sector over USD 2 trillion by 2019 (Juniper Research, 2015).

Such figures can be expected to continue to increase, especially with regard to intellectual property rights infringement. Furthermore, such reports are likely to underestimate the cost of cybercrime, as many incidents remain unreported and many companies, institutions, and individuals do not take into account (or cannot measure) the financial losses related to compromised or lost data, since they do not value data as an asset. At the same time, it is important to note that some reports of loss may be overestimated, since the cybersecurity industry is growing; in other words, investments in combating cybercrime have a positive impact on the economy. Therefore, all estimates should be approached with caution, since there is no systematic monitoring or reporting of incidents, and the academic frameworks for analysing the costs of cybercrime are still in an early phase (Anderson *et al.*, 2012). In addition to the financial losses suffered as a result of cybercrime, there are other negative effects:

- **Diminished consumer trust:** When consumers have been victims of cybercrime, without any form of redress, they tend to avoid e-commerce, which in turn has an effect on the profits of businesses. We are seeing an increasing number of successful attacks on companies' servers to acquire customers' personal data and credit card numbers, such as the collection of over 1.2 billion user-name-and-password combinations and half a billion e-mail addresses stolen in 2014 by one group from Russia (O'Toole and Pagliery, 2014). These incidents undermine user trust in online services.
- **Loss of trade secrets:** Intellectual property, such as trade secrets, is a resource of growing importance for most industries; when these trade secrets are stolen due to cybercrime, the value of their property diminishes.
- **Refusal of access to certain markets:** Many merchants refuse to carry out e-commerce transactions or even enter into new services in certain countries; Nigeria is a good example due to the numerous cases of fraudulent activities perpetrated there.
- In some cases, there could be **threats to critical infrastructure**, financial and bank systems and to national security.

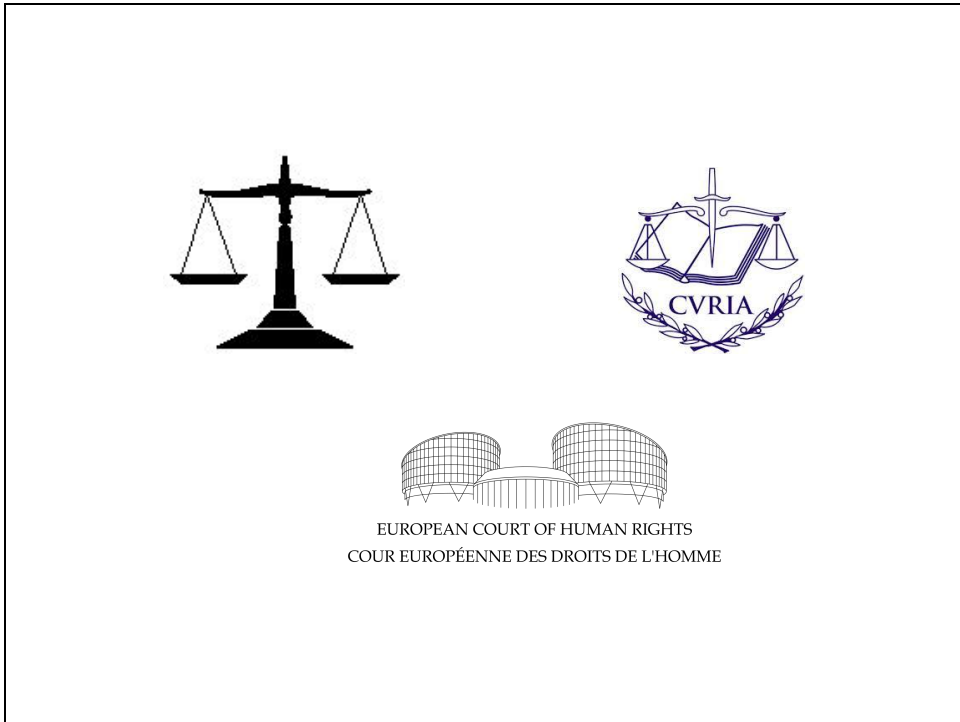
The Internet was originally designed for use by a closed circle composed mainly of academics. Communication was open and security was not an initial built-in concern. Cybersecurity came into sharper focus with the Internet's expansion beyond this circle of the Internet pioneers. The Internet reiterated the old truism that technology can be both enabling and threatening. What can be used to the advantage of society can also be used to its disadvantage.

Policy Challenges

JURISDICTION

Geneva Internet Platform

The logo for the Geneva Internet Platform, featuring a blue horizontal brushstroke underline.



The Court of Justice of the European Union (CJEU) has already played a prominent role in the rulings on the right to be forgotten, the Safe Harbour framework, and mass surveillance. This development is likely to accelerate in 2017 with national and regional courts filling digital policy gaps (lack of policy instruments to address policy issues). In 2017, the CJEU is expected to issue a ruling on whether Uber should be considered a provider of transportation or a provider of information society services. If the CJEU decides that Uber provides transportation services, the company will have to obey all rules applied to, for example, taxi companies.

In 2017, it is likely that the ruling on Microsoft by a US Appellate Court will be challenged. This landmark ruling stipulated that US authorities could not use a search warrant to force Microsoft to turn over data stored at the company's data centre in Dublin, Ireland. The ruling limits the juridical outreach of US courts over US companies with facilities abroad, an increasing practice within the Internet industry. Given the importance of the jurisdiction issue, the ultimate solution for the Microsoft case will have high relevance for future digital policy.

Courts are likely to be busy with digital issues, addressing questions of cybercrime, content removal, role of intermediaries, freedom of expression, protection of personal data, mandatory data retention requirements, and mass surveillance to name a few.

Policy Challenges

VIRTUAL CURRENCIES

Geneva Internet Platform



Unlike traditional e-money that represents fiat currency (such as EUR and USD) without changing its value, digital currency is not equivalent to any fiat currency. It is not part of a national financial system, and therefore its creation is not regulated by state authorities.

Digital currencies can be centralised or decentralised. In a centralised model, operations such as the issuance of the currency, and the mechanisms to implement and enforce rules on the use and circulation of the currency are managed by a central party. In a decentralised model, such operations are managed by various parties across the network.

Virtual currencies and cryptocurrencies are both types of digital currencies. While virtual currencies are based on a centralised model, cryptocurrencies (digital currencies that use cryptography for security, making them difficult to counterfeit) can be either centralised or decentralised. Bitcoin is one example of a decentralised cryptocurrency (Kamberi, 2014).

The European Central Bank (2012) defined virtual money (virtual currencies) as a 'type of unregulated, digital money which is issued and usually controlled by its developers, and used and accepted among the members of a specific virtual community'. According to the European Banking Authority (2014), virtual currency is 'a digital representation of value that is neither issued by a central bank or a public authority, nor necessarily attached to a fiat currency, but is accepted by natural or legal persons as a means of payment and can be transferred, stored or traded electronically'.

Cryptocurrencies are set to take the online world by storm, as their popularity and use increases. Large companies like Apple, Dell, and PayPal have already indicated their plans to

integrate cryptocurrencies as a payment method, and more are likely to follow.

In recent years, Bitcoin has emerged as one of the most popular cryptocurrencies, and the number of services that allow the use of Bitcoin has increased drastically. Many worldwide services now accept Bitcoin as payment and such transactions have been exempted from value added tax (VAT) in several countries. In July 2015, the Court of Justice of the European Union (CJEU) [ruled](#) that exchanging traditional currency for Bitcoin online should be exempt from consumption taxes just like other transactions of banknotes and coins. The court ruled that bitcoins should be treated as a means of payment, and as such were protected under the European Union directive on the common system of value added tax ([2006/112/CE](#)) exempting currency transactions from value added tax (VAT).

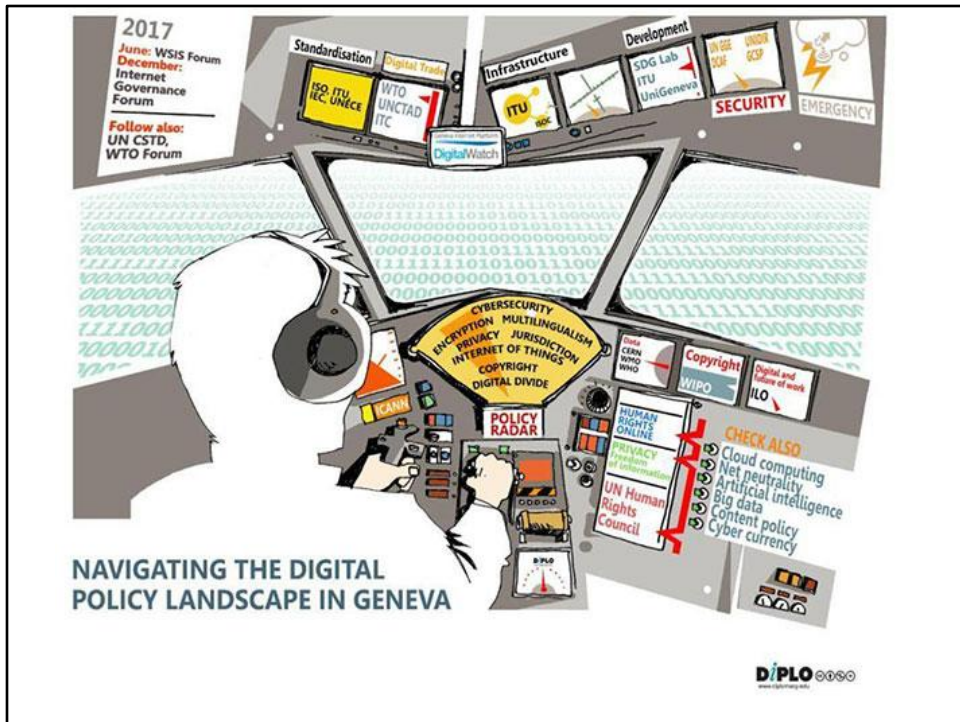
The main advantages of cryptocurrencies are low fees compared to the traditional banking system, easy mobile access, and quick and transparent methods of payment – the distributed peer-to-peer network and timestamp servers make it virtually impossible to tamper with or alter the information in a fraudulent manner. These advantages can boost the activities of start-ups and help developing countries stand on an equal footing with developed countries in the global market. In some countries where national currency faces devaluation, some citizens also see cryptocurrencies as a relatively safe way to hold their savings, although there is still uncertainty with regards to how their government will react to cryptocurrencies.

In 2016, the International Monetary Fund (IMF) published the report [Virtual Currencies and Beyond: Initial Considerations](#), which points to different challenges related to the regulation of virtual currencies, including consumer protection, taxation, and financial stability. According to the report, proper policy responses ‘will need to calibrate regulation in a manner that appropriately addresses the risks without stifling innovation’ (He *et al.*, 2016).

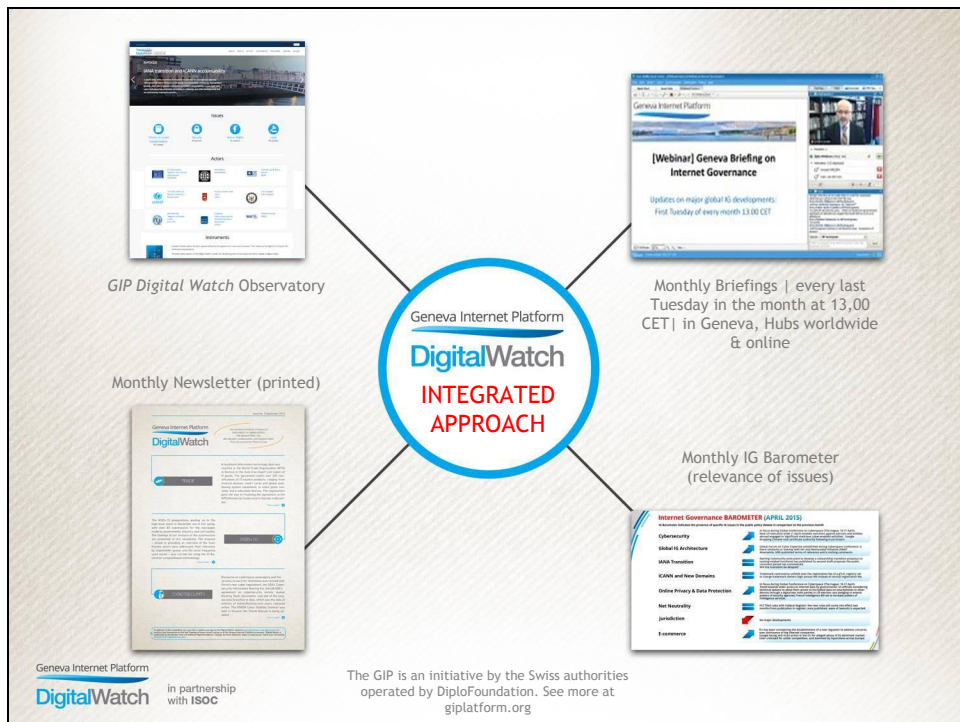
Geneva Internet Platform



How can you **benefit** from
the Geneva Internet
Platform?



The GIP helps navigate the complex and multidisciplinary digital policy scene. In particular, the GIP helps target broader policy issues such as data protection and privacy to specific contexts and needs. For example, the GIP helps 'translate' data protection policies from diplomatic language/context in Geneva to fit the needs of start-up communities worldwide. In brief, start-up communities should be aware of Geneva policy developments that can affect their business models. This is also of major concern for our company, Digita.



The GIP provides comprehensive and just-in-time reporting on digital developments. Consult the GIP Digital Watch Observatory, follow the current pressure on the digital policy IG Barometer, read the monthly newsletter summarising the key digital policy developments, and attend monthly briefings conducted every last Tuesday of the month from 13.00 to 14.00 CET.

Every Last Tuesday of the Month – Internet Governance Briefing



*You receive hundreds of pieces of information on digital politics.
We receive them, too.
We decode, contextualise, and analyse them.
Then we summarise them for you.*

This is the logic behind our monthly briefings. You can add the last Tuesday of the month to your calendar and join us for [monthly briefings](#). In these hour-long briefings, you will get an overall picture of digital developments of relevance for you.

Every Last Tuesday of the Month – Internet Governance Briefing

The screenshot displays a video conference interface. The main content area shows a slide with the following text:

- Regional updates
- Local hubs & regional perspectives
- Geneva Internet Platform D/PLO
- 23 February 2016 | 18

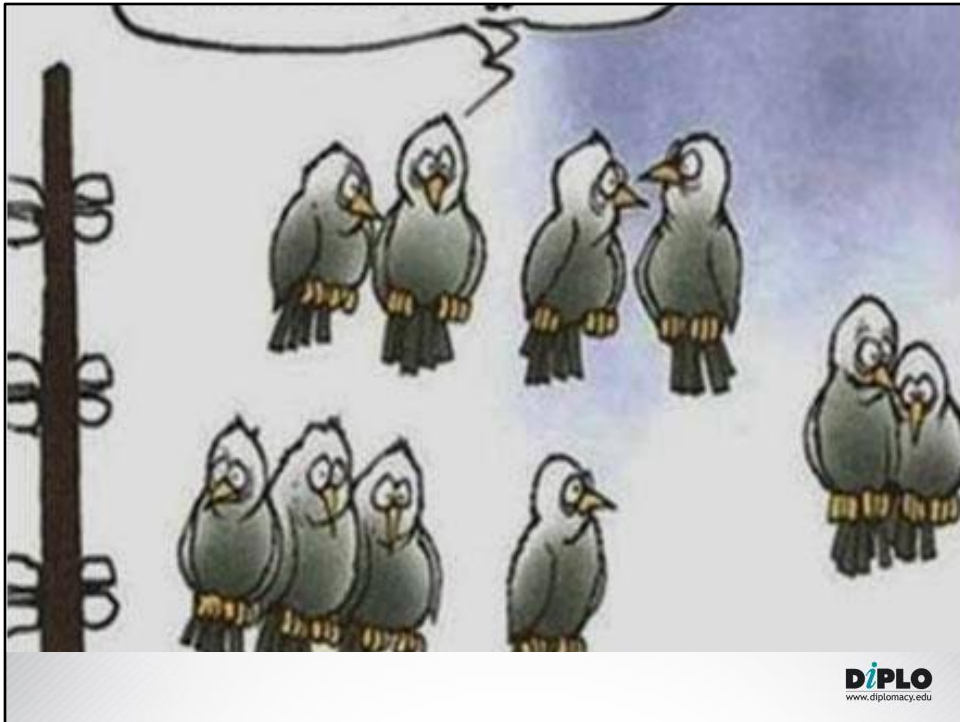
The interface also includes a chat window at the bottom left with the following messages:

- Michael Oglio: I don't know that about Tunisia Horras, thanks for the info
- Horras Ben Walid: Telco and ISP allowed differential prices for pricing, this was about by activists in India...
- Charles Ben Romdhane: sorry but the word 'get away'?
- Horras Ben Walid: Michael more on <http://www.geneva.org/index.php/19/32>
- Emmanuel Sacchetti: Sorry Chéri, hope is better now
- Kalimuddin: India... I am from Arab
- Horras Ben Walid: I wrote about mapping VoIP blacklogs in the MENA Region...
- Michael Oglio: Awesome! Thanks Horras!
- Emmanuel Sacchetti: really interesting Horras, thank you
- Michael Oglio: Yes, I follow on LinkedIn, but missed this one :)
- Kalimuddin: gpccommunity

On the right side, there are video thumbnails for participants and a list of attendees including: #gipforum Geneva, #gipforum MENA, #gipforum Africa, #gipforum Asia, #gipforum Europe, #gipforum Latin America, #gipforum Middle East, #gipforum Oceania, #gipforum South America, #gipforum Africa, #gipforum Asia, #gipforum Europe, #gipforum Latin America, #gipforum Middle East, #gipforum Oceania, #gipforum South America.

Monthly briefings start with a global survey of digital developments and continue with regional and national developments. Here is a typical schedule of monthly briefing:

- 13.00 – 13.20 Global perspective: main digital policy developments
- 13.20 – 13.40 Regional perspectives: round-up from GIP hubs worldwide
- 13.40 – 14.00 Local developments: discussion at the local hubs on national and other local digital initiatives



... and be ready for the counter-intuitive in this digital policy journey.



- **Web:** <http://dig.watch>
- **Twitter:** @jovankurbalija
- **Email:** jovank@diplomacy.edu