Internet Governance for Libraries

A Guide to the Policies and Processes behind the Internet and their Impact
Part 5: Legal, Economic and Security Issues in Internet Governance

Part 5 of IFLA's Guide on Internet Governance for Libraries focused on societal questions – primarily discussions around regulation of online content and multilingualism. This part continues the discussion of different themes and debates that often feature in internet governance debates.

Legal Issues

The fact of talking about internet 'governance' implies that decisions are being made about the way the internet operates – in short, it is not completely anarchic. Indeed, in the case of basic standards, the fact of having rules and protocols is essential for the Internet to work at all.

But going beyond this, almost all will recognise that, just as in the physical world, laws are needed. There is a precedent for this also, with a body of law emerging around telecommunications and other information providers over previous centuries.

Therefore, rather than trying to invent new rules for the internet, there appears to be consensus around the idea that the same laws should apply. The focus, then, is rather on how to enforce these rules, given that they may need to be adapted for this new environment.

National vs International

National legislators continue to be the most active in taking steps to regulate the Internet. Emerging issues and concerns will therefore, first of all, tend to lead to national reforms, for example in order to promote privacy and data protection, protect intellectual property, enforce taxation, or tackle cybercrime.

However, given that the internet works across borders, there are limits to the effectiveness of national laws. For example, a cybercrime law in country A may struggle to inflict punishment on a criminal in country B.

As a result, there are moves to use international public law as a means of addressing challenges online which affect more than one jurisdiction. International public laws that already deal with matters relevant to Internet Governance include the ITU's International Telecommunication Regulations (ITRs) and the Council of Europe Convention on Cybercrime. Both of these are legally binding. Other aspects of international public law could also be applicable, including key principles that have been tried and tested already.

Alternative Responses

Some suggest that, rather than allowing national governments to do as they will, or trying to sign treaties, it would be best to work towards a harmonisation of national laws. This could start with issues where there is already a level of consensus, such as child sexual abuse. However, there are limited examples of this sort of work succeeding for now. More likely, perhaps, is the fact that a legal standard adopted by a major country or group of countries will serve as an example to others. Arguably, this is the case with the General Data Protection Regulation for example.

Clearly a key function of the law is to help resolve disputes – who is right and who is wrong. Even when a law exists, international courts are often slow and may not be well suited to internet related cases. A different option is Alternative Dispute Resolution (ADR), which uses arbitration and mediation amongst other tools to find solutions.

Organisations like ICANN have used these tools extensively already, and in 2016 the European Union also launched an online dispute resolution tool for consumers in disagreements about contracts. There are also suggestions that private companies should provide these services as a more efficient means of finding answers than going to court.

Finally, there is some evidence of growing pressure on internet platforms to regulate themselves. From a practical point of view, this may be inevitable, as governments often do not have the resources themselves. However, it implies private companies taking on the role of regulators of free speech and information access, as highlighted in a report of the UN Special Rapporteur on Freedom of Expression in 2018.

The Case of Copyright

Copyright represents a particularly well-discussed case. The internet has undoubtedly had a major impact here, both in terms of facilitating copying and sharing of works, and in the degree of control that rightholders can continue to exercise over use.

This is an area where there have been international efforts to legislate, notably through the WIPO Internet Treaties of 1996 (the WIPO Copyright Treaty and WIPO Performances and Phonograms Treaty), which in turn led to legislation such as the Digital Millennium Copyright Act (DMCA) in the US, and EU e-Commerce and InfoSoc Directives. Trade deals have also incorporated copyright-related provisions.

A key issue in such legislation is that laws have tended to focus more on creating rights, rather than on the exceptions and limitations that allow libraries to do their jobs. For example, these laws tend to offer legal protection to Technological Protection Measures (Digital Rights Management) that can gather data and prevent uses, even when these are legitimate. End user agreements can have the same effect. Meanwhile, even when there are provisions about exceptions and limitations, these are often optional rather than mandatory.

At the same time, the WIPO Internet Treaties allowed space for the concept of safe harbour – protection for platforms and other intermediaries such as Internet Service Providers against liability for infringing content uploaded by users without their knowledge. This features in the US and European legislation, as well as in a number of cases, for example Scarlet v SABAM in the European courts and the Scientology case in the Netherlands, plus RIAA v Verizon in the US.

While, arguably, the idea of safe harbour has been crucial in allowing the internet to realise its potential as a space for sharing and co-creating, there are criticisms. The dominance of a few major players has focused attention, with safe harbour seen by some as giving them an (unfair) advantage in negotiations with others. As such, there are growing efforts to restrict this principle, not only in the context of copyright protection, but also as part of anti-terrorist laws.

Case Study: European Copyright Reform

The ongoing discussion about the European Union's draft Directive on Copyright in the Digital Single Market provides an illustration of the different debates around this subject at the moment.

On the positive side, there is an acceptance that exceptions can support growth and public interest goals by dealing with market failure. For this potential to be realised, it is important for exceptions both to be harmonised across borders, and protected from override by contract terms or technological protection measures. This is the case with new rules around text and data mining and preservation, as well as (to some extent) access to out-of-commerce works.

On the negative side, there are both new rights for the use of small snippets of news stories on aggregator sites (Article 11), and tough restrictions on internet platforms, which are justified as a means of fighting piracy (Article 13).

The new rights, which already failed when applied at a national level in Germany and Spain, seem to have little evidence to justify their creation. Indeed, they may end up hurting smaller newspapers which rely on traffic from aggregators to earn advertising revenue.

Meanwhile, Article 13 seeks to make platforms themselves liable for content uploaded by users, forcing them to apply automated filters. For the reasons already set out in Part IV of this guide, this is problematic from a human rights point of view. In the end, Articles 11 and 13 are (clumsy) attempts to use copyright laws to tackle problems which are more associated with competition. We still hope that this provision can be dropped.

Economic Issues

The Internet has clearly has an important economic dimension. Specific issues include E-commerce, E-banking, the internet data economy and the economics of internet access.

E-commerce refers to commercial transactions conducted through the Internet, be they business to consumer (B2C), business to business (B2B), business to government (B2G) or consumer to consumer (C2C). There is considerable interest in E-commerce as a means of giving more producers, including from developing countries, access to markets without having to pass through traditional distribution and sales networks.

Nonetheless, as with traditional commerce, concerns about fraud, theft and consumer rights also apply online, leading to efforts to find solutions and build confidence. As a result, individual countries and regions are developing their own frameworks for addressing eCommerce concerns, although of course these are only fully effective when both buyer and seller are based within their jurisdiction.

At the global level, the World Trade Organisation (WTO) is the leading body that regulates international trade for goods (through GATT), services (though GATS) and intellectual property rights (IPRs) (through TRIPS). As a result, many important e-

commerce issues (goods and services but also telecommunication liberalisation and IPR, among others) are on its agenda.

There is talk of a more focused effort on the subject, with 76 Member States launching talks in January 2019. These will explore whether GATT and GATS rules need to be adapted or changed (for example, if you purchase a book online comprising a hard copy and a digital file, which rules should apply) as well as how to deal with questions around data localisation and fighting spam, amongst other things.

An additional concern is about the relationship between WIPO and WTO rules. While WIPO is traditionally the guardian of rules around Intellectual Property, it has no international dispute settlement mechanism to enforce them, as is the case of the WTO.

In addition to WTO and WIPO, there are other regional and global initiatives that deal with e-commerce. For example, there is Electronic Business XML, a project to use Extendable Markup Language to standardise the secure exchange of business data. As highlighted, there are regional initiatives, such as the European Union's E-commerce Directive, the APEC blueprint for action on e-commerce for the Asia pacific region and the Common Market for Eastern and Southern Africa (COMESA).

E-banking refers to the ability to conduct banking-related transactions via the internet. This has allowed for many more people to open bank and payment accounts, even when there is no bank locally, supporting financial inclusion.

The internet has also been behind the development of digital currencies, including virtual or cryptocurrencies, which seek to bypass traditional banks altogether. These currencies, of which the most famous example is Bitcoin, work by using a 'distributed ledger' technique. By having many copies of transactions, held in different places, it makes it almost impossible to defraud the system. They operate on trust, with value set by levels of investor interest. Increasingly, however, other actors (including banks) are experimenting with this technology in order to benefit from the gains for security and trust.

Cryptocurrencies have increased in popularity over the years and are likely to remain a key part of economic discussions around the Internet. PayPal and Apple are planning to integrate cryptocurrencies as a payment alternative in upcoming years.

The Internet Data Economy refers to new business models that have emerged as a result of the ability of people and organizations to collect and use data, primarily for the purposes of advertising.

With more data about consumer behaviour implying more value, there is a trend towards monopoly power, with major platforms offering a variety of services able to collect unparalleled amounts of information. This data can then be used or sold on for advertising purposes (including political advertising, as the Cambridge Analytica scandal showed), or used in order to favour one service over another.

In terms of regulation, the European Union has perhaps been the most active, with efforts around competition (for example, to prevent Google from giving its Shopping

pages preference in search results), and encourage consumers to understand how their data is used and take conscious decisions about this.

The economics of internet access refers to the economy that has grown up around how internet connectivity and access to data is paid for. There is a tension, with internet service providers sometimes arguing that they should benefit from the revenues of major content providers, given that is it their cables and masts that are bringing it to customers. Without a more revenue, they will not be able to invest in higher quality services.

Indeed, this has been suggested by the European Telecommunication Operators (ETNO), which suggested Google and Facebook should pay them. Content suppliers, of course, have argued that without what they provide, there would be lower demand for Internet connections. Moreover, in a number of countries, there are concerns about level of competition in the ISP sector, which can itself lead to excessive prices and under-investment.

A further issue is the asymmetry of fees between advanced and developing economies. Given that it is the user who bears all of the costs of connection, they can risk having to subsidise the building 'backbone' connections to exchange points in developed countries, to the benefit of the latter. This contrasts with the situation for international phone-calls, where companies in developing countries would at least benefit from some of the fees for calls.

Security Issues

The internet is now recognised as an example of critical infrastructure, essential for many aspects of daily life. In order to allow economies and societies to function, it therefore needs to be protected, and vulnerabilities identified and managed.

There are various ways in which the internet, or individual sites, can be attacked, as set out in the DIPLO guide on Internet Governance. This sets out three basic classification criteria for cybersecurity issues.

Type of action: Classification based on type of action may include data interception, data interference, illegal access, spyware (or malware – software that disrupts, damages, or gives unauthorized access to a computer system), botnets (a network of private computers infected with malicious software and controlled as a group without the owners' knowledge) data corruption, sabotage, denial-of-service (DoS – a coordinated effort to flood a site or service and so disable it), and identity theft (often through 'phishing').

Type of perpetrator: Possible perpetrators might include criminals, anarchists, hacktivists, revolutionaries, terrorists, secret services, and defence and military units.

Type of target: Potential targets are numerous, ranging from individuals, private companies, civil society organisations, media entities, and public institutions, to core Internet infrastructure (telecom operators, ISPs, IXPs, data centres), critical society infrastructures (power and water supplies, industry facilities, traffic, etc.), and military assets.

There are efforts to implement regulations and policies at a global and regional level to maintain and improve cybersecurity. The United Nations has a Group of Governmental Experts (UN GGE) that has had a mandate since 2004 to work in the field of information security. The UN Office on Drugs and Crime (UNODC) is also very active in fighting cybercrime.

As a result of the WSIS 2005 agenda, the international Telecommunication Union (ITU) has launched several activities on cybersecurity such as the Global Cybersecurity Agenda (GCA) and the Global Cybersecurity Index (GCI).

NATO adopted a Policy on Cyber Defence in 2014 and spearheaded the initiative to apply international law to cyberspace through the adoption of the Tallinn Manual on the International Law Applicable to Cyber Warfare.

At the regional level, Europe has addressed cybersecurity through the 2004 Convention on Cybercrime of the Council of Europe. The OSCE also works on cybersecurity and developed a set of confidence-building measures (CBMs) in the fight against cybercrime.

In 2003, the Organization of American States (OAS) set up the Inter-American Cyber-Security Strategy, which includes the efforts of three groups of the organisation: the Inter-American Committee against Terrorism (CICTE), Ministers of Justice or Other Ministers or Attorneys General of the Americas (REMJA), and the Inter-American Telecommunication Commission (CITEL). In Africa, cybersecurity policy has centred on drafting the African Union Convention on Cyber Security and Personal Data Protection.

Nonetheless, the issue of cybersecurity has not gone away, and with new threats and techniques emerging regularly, it remains a major topic of discussion at the Internet Governance Forum.