|  |  |
| --- | --- |
|  | **Addendum 15 to Document EG-ITRs-1/2** |
| **7 September 2023** |
| **English only** |
|  |  |
| Contribution from HILL | |
| NEW TRENDS IN TELECOMMUNICATIONS/ICT AND EMERGING ISSUES IN INTERNATIONAL TELECOMMUNICATIONS/ICT ENVIRONMENT WHICH MAY IMPACT THE ITRS | |
| **Purpose**  Discussion  **Action required**  The document is submitted to EG-ITRs **for discussion**.  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  **Reference**  [Council Resolution 1379, revised 2023](https://www.itu.int/md/S23-CL-C-0121/en) | |

1. The work of the current ITR-EG is specified in its Terms of Reference[[1]](#footnote-1):

*2 Taking into consideration the work of the previous two Expert Groups, the review may consider, among others:*

*a) new trends in telecommunications/ICT and emerging issues in international telecommunications/ICT environment which may impact the ITRs,*

*b) empirical data on the current use of the ITRs by operating agencies and/or administrations and the proportion of global telecommunication services which now rely on the ITRs, and*

*c) the relevance of the ITRs which “consist of high-level guiding principles” in the current telecommunication/ICT environment.*

2. This contribution focuses on new trends in telecommunications/ICT and emerging issues in international telecommunications/ICT environment which may impact the ITRs.

What follows is essentially identical to the essay “[A New Convention for Data and Cyberspace](https://itforchange.net/digital-new-deal/2020/10/30/a-new-convention-for-data-and-cyberspace/)”, in the call for a [Digital New Deal](https://itforchange.net/digital-new-deal/) (October 2020).

It includes issues that have been addressed in other addendums. They are included here to show the structure and scope of what should be considered for inclusion in new treaty provisions.

**Abstract**

The time has come for the international community to negotiate and agree to a new treaty – a Convention for Data and Cyberspace – which would contain explicit principles for extending well-established offline legal frameworks and principles to the online world, particularly with respect to certain key domains. There would appear to be wide support for such a treaty, given that many countries have come together, in the context of trade negotiations, to constitute treaty provisions covering specific areas. However, trade negotiations are an inherently inappropriate forum to develop such provisions, given their secretive, undemocratic nature and their susceptibility to lobbying by large private companies. Deliberations on such a new treaty need not be a prolonged process, since the goal is merely to transpose to the online world principles that are already well accepted offline. There is a regular treaty-making mechanism, the ITU Plenipotentiary Conference, that takes place every four years. This forum could conveniently be used for the process of negotiating the kind of treaty being proposed here.

**1. Introduction**

Just as the proliferation of steam power and mechanization inaugurated the industrial age three centuries ago, the growing centrality of data and associated technologies are poised to dramatically revolutionize the nature of social and economic life today. As in the early years of industrialization, we once again find ourselves in the midst of a frenzied race to capitalize on these new technologies, and the frameworks that will organize and control them. The issue of international governance is thus of paramount importance. As Roger Brownsword puts it:

“… what happened to us over the last 20 years is that, both publicly and privately, we have become increasingly reliant on information technologies (creating new kinds of vulnerability, both collective and personal), we have migrated many routine activities to on-line environments in ways that are deeply disruptive (we live for many hours each day in our on-line worlds), and we have begun to appreciate that the technological management of our activities has major regulatory implications. If we want to retain a degree of control over our futures, then we need to exert some influence over the spheres of regulatory significance – which is to say, we need to work on creating the right kind of regulatory environment not only for information technologies but also for a raft of other technologies that are enabled by information technology and that are converging to shape our futures.”

While numerous efforts have been made to achieve such a regulatory environment in the national context, the nature of the internet and information technology, as well as the economic activities built around them, require more broad-based interventions. This, unfortunately, has been made difficult by the vested interests of hegemonic powers, as well as the contested terrain of international law. Indeed, as noted elsewhere[1](https://projects.itforchange.net/digital-new-deal/2020/10/30/a-new-convention-for-data-and-cyberspace/#article-footnote-368-1), the current order of global governance is arguably similar to that of feudal Europe, where multiple arrangements of decision-making including the Church, cities ruled by merchant-citizens, kingdoms, empires, and guilds co-existed with little agreement on who held charge over a given territory or subject.

Within this tangled system, internet governance has evolved under the rubric of what is called ‘the multistakeholder model’. Couched in a discourse that promotes egalitarian values and greater participation, this model[2](https://projects.itforchange.net/digital-new-deal/2020/10/30/a-new-convention-for-data-and-cyberspace/#article-footnote-368-2) has, in reality, been employed as a means to circumscribe the power of national governments (and intergovernmental organizations) vis-à-vis private transnational corporations. It has fostered not only a strikingly undemocratic regime, but also one that has been dominated by the geopolitical and economic interests of the United States. Be it for the vast unilateral surveillance apparatus that it has built, or the added advantage of its Silicon Valley behemoths, the US has continually worked to ensure that the governance of internet-based technologies remains firmly in its control even as it has postured towards allowing others – but not other governments – to take charge. Furthermore, recent developments in international negotiations point towards accelerated efforts to have large parts of the international community ‘locked in’ to agreements that mandate a liberalized regime involving little regulatory oversight and free flow of data across borders.

This essay argues that the international community needs to not accede to these prevailing trends. There is ample scholarship produced over the years that explores alternative modes of internet governance which may be built upon to craft a democratic and thoughtful regulatory framework that addresses the needs and concerns of a wide variety of actors.

Many in the international community are beginning to realize the importance of regulatory provisions for the digital sphere, and are more open to discussing them in the context of trade negotiations. While the recognition that such issues must be discussed in an intergovernmental forum is a positive sign, trade negotiations are an inherently inappropriate forum for such talks given their secretive, undemocratic nature and their susceptibility to lobbying by large private companies. Of course, there is likely to be inertia and pushback from the powers that be. But this is precisely because they have a lot to lose from any ‘fragmentation’ of the internet that shuts them out from access to large markets and sources of data. If the rest of the international community can come together, it is possible to force them into a reasonable agreement.

The time has come to initiate negotiations for a new treaty – let us call it a Convention for Data and Cyberspace – as a first step towards ushering in a rational and equitable global internet governance regime. It will contain explicit principles for extending well-accepted offline law to the online world, with specific emphasis on key domains. Given the current international environment, there ought to be considerable support for such an initiative. Moreover, there is sufficient consensus on fundamental legal principles in offline law to have them form a foundation for ordering the governance of the digital world.

The essay will begin by outlining fifteen key areas (sections 1.1 to 1.15) of well-established offline law that are undeveloped or not deployed at all in the digital realm, briefly touching upon the key points that need to be considered when developing and transposing these legal frameworks. Section 2 will argue for a new treaty and make concrete proposals for what it may look like. Finally, drawing on the pioneering work of the Just Net Coalition (a network of civil society organizations from around the world), sections 3.1 to 3.11 will set out the principles and provisions that could constitute this treaty and form the bedrock for a new epoch in internet governance.

The fifteen key areas mentioned above are:

1. Democratic control over key online issues and decisions

2. Infrastructure, such as access to the internet, email, and directories

3. Freedom from unwarranted restrictions on freedom of speech (censorship is delegated to unaccountable private companies)

4. Provision of reliable information and protection against defamation

5. Privacy of communications

6. Protection of personal data

7. Security standards required to correct market failures due to information asymmetries and externalities

8. Curbing abuse of dominant market power that arises because of network effects and economies of scale

9. Refraining from producing, procuring, and/or stockpiling dangerous technologies that will inevitably fall into the hands of ill-intentioned actors

10. Equitable taxation of digital services

11. Equitable distribution of the value-added of a newly-discovered natural resource: Data

12. Equitable application of labor laws for online work

13. Equitable application of consumer protection laws for online transactions

14. Equitable distribution of the value of intellectual property rights

15. Efficacy and safety of new technologies such as artificial intelligence

**1.1 Democratic control over key online issues and decisions**

The importance of democratic control over internet governance at the national level was recognized more than 20 years ago. As Zoe Baird notes:

“In the early years of internet development, the prevailing view was that government should stay out of internet governance; market forces and self-regulation would suffice to create order and enforce standards of behavior. But this view has proven inadequate as the internet has become mainstream. A reliance on markets and self-policing has failed to address adequately the important interests of internet users such as privacy protection, security, and access to diverse content. And as the number of users has grown worldwide, so have calls for protection of these important public and consumer interests. It is time we accept this emerging reality and recognize the need for a significant role for government on key internet policy issues.”

Similar considerations hold at the international level too. Indeed, as the UK Conservative Party put the matter in its 2017 Manifesto:

“The internet is a global network and it is only by concerted global action that we can make true progress.

We believe that the United Kingdom can lead the world in providing answers. So we will open discussions with the leading tech companies and other like-minded democracies about the global rules of the digital economy, to develop an international legal framework that we have for so long benefited from in other areas like banking and trade. We recognize the complexity of this task and that this will be the beginning of a process, but it is a task which we believe is necessary and which we intend to lead.

By doing these things – a digital charter, a framework for data ethics, and a new international agreement – we will put our great country at the head of this new revolution; we will choose how technology forms our future; and we will demonstrate, even in the face of unprecedented change, the good that government can do.”

These statements implicitly recognize that current arrangements for the governance of the internet (the so-called multistakeholder model) are not adequate.[3](https://projects.itforchange.net/digital-new-deal/2020/10/30/a-new-convention-for-data-and-cyberspace/#article-footnote-368-3) Unfortunately, there has been little progress to date with respect to establishing democratic control.[4](https://projects.itforchange.net/digital-new-deal/2020/10/30/a-new-convention-for-data-and-cyberspace/#article-footnote-368-4)

**1.2 Infrastructure, such as access to the internet, email, and directories**

The state has always been implicated in the creation of large scale social and economic infrastructure. Many nations and empires, for instance, have built and maintained roads in order to facilitate communication networks such as the postal service. The early development of the internet was funded by governments as well.[5](https://projects.itforchange.net/digital-new-deal/2020/10/30/a-new-convention-for-data-and-cyberspace/#article-footnote-368-5)

It is thus surprising that most governments do not mandate, by law or regulation, that affordable internet access, including email and basic directory services, be made available to all. Given that all governments ensure (or strive to ensure) affordable access to roads, water, electricity, sewage disposal, physical mail, etc., why shouldn’t they ensure (or strive to ensure) affordable access to the internet and email? Indeed, a 2018 United Nations (UN) resolution implicitly urges states to ensure universal and affordable access.[6](https://projects.itforchange.net/digital-new-deal/2020/10/30/a-new-convention-for-data-and-cyberspace/#article-footnote-368-6)

We can also question why states should implicitly, and without democratic control, delegate the rollout of affordable internet access infrastructure to private companies, particularly dominant social media platforms. No justification is forthcoming on this point. Yet, this is a worrisome and growing trend. Indeed, as one researcher puts it, “That corporations which are already gatekeepers of internet content are increasingly becoming caretakers of its backbone infrastructures raises questions of transparency, accountability, and undemocratic concentration of power.”[7](https://projects.itforchange.net/digital-new-deal/2020/10/30/a-new-convention-for-data-and-cyberspace/" \l "article-footnote-368-7)

**1.3 Freedom from unwarranted restrictions on freedom of speech (censorship is delegated to unaccountable private companies)**

It is universally accepted that freedom of speech is a basic right, and that the right applies equally online.[8](https://projects.itforchange.net/digital-new-deal/2020/10/30/a-new-convention-for-data-and-cyberspace/#article-footnote-368-8) There is also universal “concern about the spread of disinformation and propaganda on the internet, which can be designed and implemented so as to mislead, violate human rights and privacy, and incite violence, hatred, discrimination, or hostility”.[9](https://projects.itforchange.net/digital-new-deal/2020/10/30/a-new-convention-for-data-and-cyberspace/#article-footnote-368-9)

It has long been understood that, in a democratic society, restrictions on freedom of speech can only be imposed by law, and that government actions to restrict freedom of speech must be subject to review by impartial and independent tribunals.[10](https://projects.itforchange.net/digital-new-deal/2020/10/30/a-new-convention-for-data-and-cyberspace/#article-footnote-368-10)

However, dominant social media platforms exercise de facto censorship based on unilaterally imposed “standards of conduct”. Since platforms are private entities, they can publish – or not – what they see fit, without any judicial oversight (except for allegations of copyright infringement, defamation, or other illegal activities).[11](https://projects.itforchange.net/digital-new-deal/2020/10/30/a-new-convention-for-data-and-cyberspace/#article-footnote-368-11)

The current regime, particularly in the US, is perceived as giving too much power to social platforms to control what is or is not published, in effect restricting freedom of speech.[12](https://projects.itforchange.net/digital-new-deal/2020/10/30/a-new-convention-for-data-and-cyberspace/#article-footnote-368-12)

**1.4 Provision of reliable information and protection against defamation**

As noted above, the current regime results in the publication of a great deal of misleading or downright incorrect information. Further, the limited liability of intermediaries makes it difficult to remove defamatory material: since the dominant platforms are based in the US, a “victim” must file a lawsuit in the US in order to force a platform to remove such material. This is not consistent with offline law, according to which victims of defamation can, under certain conditions, file lawsuits in their own country.

**1.5 Privacy of communications**

It is universally accepted that online privacy is important and that technical solutions such as encryption can be a critical means to ensure such privacy.[13](https://projects.itforchange.net/digital-new-deal/2020/10/30/a-new-convention-for-data-and-cyberspace/#article-footnote-368-13) There is also universal concern about “the arbitrary or unlawful collection, retention, processing, and use or disclosure of personal data on the internet”.[14](https://projects.itforchange.net/digital-new-deal/2020/10/30/a-new-convention-for-data-and-cyberspace/#article-footnote-368-14)

Existing international law is out of date and does not provide sufficient protection for the privacy of communications.[15](https://projects.itforchange.net/digital-new-deal/2020/10/30/a-new-convention-for-data-and-cyberspace/#article-footnote-368-15)

**1.6 Protection of personal data**

It is universally recognized that unlawful or arbitrary collection of personal data is a highly intrusive act, which may violate the right to privacy.[16](https://projects.itforchange.net/digital-new-deal/2020/10/30/a-new-convention-for-data-and-cyberspace/#article-footnote-368-16) There is also a universal concern about “the negative impact that surveillance and/or interception of communications, including extraterritorial surveillance and/or interception of communications, as well as the collection of personal data, in particular when carried out on a mass scale, may have on the exercise and enjoyment of human rights.”[17](https://projects.itforchange.net/digital-new-deal/2020/10/30/a-new-convention-for-data-and-cyberspace/#article-footnote-368-17) That surveillance is carried out not just by governments (in the interest of national security) but also by private companies for commercial purposes,[18](https://projects.itforchange.net/digital-new-deal/2020/10/30/a-new-convention-for-data-and-cyberspace/#article-footnote-368-18) and such private surveillance may have negative national security implications.[19](https://projects.itforchange.net/digital-new-deal/2020/10/30/a-new-convention-for-data-and-cyberspace/#article-footnote-368-19)

Members of the Council of Europe, and some other states, have addressed this issue by adopting the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. The European Union has gone further, adopting the General Data Protection Regulation (GDPR).

But apart from these regional instruments, existing international law is out of date and does not provide sufficient protection for data privacy.[20](https://projects.itforchange.net/digital-new-deal/2020/10/30/a-new-convention-for-data-and-cyberspace/#article-footnote-368-20)

**1.7 Security standards required to correct market failures due to information asymmetries and externalities**

Security experts have long recognized that the lack of information and communication technology (ICT) security creates a negative externality.[21](https://projects.itforchange.net/digital-new-deal/2020/10/30/a-new-convention-for-data-and-cyberspace/#article-footnote-368-21) For example, if an electronic commerce service is hacked and credit card information is disclosed, the users of the service will have to change their credit cards. This is a cost both for the end user and the credit card company. However, that cost is not visible to the e-commerce service. Consequently, the service does not have an incentive to invest in greater security measures. Furthermore, users do not have the information or the technical expertise required to determine whether any particular product or service has adequate security. That is, there is an asymmetry of information in which the supplier knows more than the customer.[22](https://projects.itforchange.net/digital-new-deal/2020/10/30/a-new-convention-for-data-and-cyberspace/#article-footnote-368-22)

Such market failures can only be corrected by regulatory action, specifically, by imposing liability on suppliers of insecure devices and/or mandating minimum security standards. This is the case for airplanes, automobiles, electrical appliances, pharmaceuticals, etc. Why should it not be the case for ICTs?[23](https://projects.itforchange.net/digital-new-deal/2020/10/30/a-new-convention-for-data-and-cyberspace/#article-footnote-368-23)

**1.8 Curbing abuse of dominant market power that arises because of network effects and economies of scale**

It is an observed fact that, for certain services (for example, internet searches, social networks, online book sales, online hotel reservations, etc.) one particular provider becomes dominant.[24](https://projects.itforchange.net/digital-new-deal/2020/10/30/a-new-convention-for-data-and-cyberspace/#article-footnote-368-24) If the dominance is on account of better services, then market forces are at work and there is no need for regulatory intervention.

However, if the dominance is due to economies of scale and network effects,[25](https://projects.itforchange.net/digital-new-deal/2020/10/30/a-new-convention-for-data-and-cyberspace/#article-footnote-368-25) then a situation akin to a natural monopoly might arise, leading to abuse of dominant market power.[26](https://projects.itforchange.net/digital-new-deal/2020/10/30/a-new-convention-for-data-and-cyberspace/#article-footnote-368-26) For example, platforms might abusively use personal data to set high prices of goods for certain customers,[27](https://projects.itforchange.net/digital-new-deal/2020/10/30/a-new-convention-for-data-and-cyberspace/#article-footnote-368-27) a dominant national provider might impede the operation of an international competitor,[28](https://projects.itforchange.net/digital-new-deal/2020/10/30/a-new-convention-for-data-and-cyberspace/#article-footnote-368-28) a dominant company may excessively influence governments,[29](https://projects.itforchange.net/digital-new-deal/2020/10/30/a-new-convention-for-data-and-cyberspace/#article-footnote-368-29) or a dominant search engine might provide search results that favor certain retail sites.[30](https://projects.itforchange.net/digital-new-deal/2020/10/30/a-new-convention-for-data-and-cyberspace/#article-footnote-368-30)

In such cases, regulatory intervention is certainly required. Yet, enforcement of national competition law is inadequate,[31](https://projects.itforchange.net/digital-new-deal/2020/10/30/a-new-convention-for-data-and-cyberspace/#article-footnote-368-31) particularly in the US,[32](https://projects.itforchange.net/digital-new-deal/2020/10/30/a-new-convention-for-data-and-cyberspace/#article-footnote-368-32) and there is no international competition law.[33](https://projects.itforchange.net/digital-new-deal/2020/10/30/a-new-convention-for-data-and-cyberspace/#article-footnote-368-33)

**1.9 Refraining from producing, procuring, and/or stockpiling dangerous technologies that will inevitably fall into the hands of ill-intentioned actors**

Some recent, and very dangerous, cyberattacks were based on malware that was stockpiled by a government (for its own potential cyberwarfare), but fell into criminal hands.[34](https://projects.itforchange.net/digital-new-deal/2020/10/30/a-new-convention-for-data-and-cyberspace/#article-footnote-368-34) This is not acceptable. As stated in 2017 by the Microsoft president:[35](https://projects.itforchange.net/digital-new-deal/2020/10/30/a-new-convention-for-data-and-cyberspace/#article-footnote-368-35)

“The time has come to call on the world’s governments to come together, affirm international cybersecurity norms that have emerged in recent years, adopt new and binding rules, and get to work implementing them.”

“Such a [set of binding rules set forth in a] convention should commit governments to avoiding cyberattacks that target the private sector or critical infrastructure or the use of hacking to steal intellectual property. Similarly, it should require that governments assist private sector efforts to detect, contain, respond to, and recover from these events, and should mandate that governments report vulnerabilities to vendors rather than stockpile, sell, or exploit them.”

**1.10 Equitable taxation of digital services**

At present, multinational companies in general, and ICT companies in particular, minimize (or even avoid) tax payments by structuring their operations to take advantage of the differences in tax laws in different countries.[36](https://projects.itforchange.net/digital-new-deal/2020/10/30/a-new-convention-for-data-and-cyberspace/#article-footnote-368-36) As a result, many ICT companies pay little or no tax. Since most activities are moving online, this can result in a significant loss of revenue for states, impeding their ability to provide basic services to their citizens. Further, it is important to recall that large companies are the main beneficiaries of various forms of state aid: subsidies, state-funded research and development, initiatives to favor exports, infrastructure such as roads and electricity, etc.

**1.11 Equitable distribution of the value-added of a newly-discovered natural resource: data**

It is obvious that personal data has great value when collected on a mass scale and cross-referenced.[37](https://projects.itforchange.net/digital-new-deal/2020/10/30/a-new-convention-for-data-and-cyberspace/#article-footnote-368-37) Indeed, the monetization of personal data drives both internet services and the provision of so-called free services such as search engines.[38](https://projects.itforchange.net/digital-new-deal/2020/10/30/a-new-convention-for-data-and-cyberspace/#article-footnote-368-38)

Yet, at present, there are no laws or regulations that would ensure an equitable distribution of the value-added of data. On the contrary, the entire value-added is captured by a handful of dominant companies.[39](https://projects.itforchange.net/digital-new-deal/2020/10/30/a-new-convention-for-data-and-cyberspace/#article-footnote-368-39) This is not sustainable.

A recent study[40](https://projects.itforchange.net/digital-new-deal/2020/10/30/a-new-convention-for-data-and-cyberspace/#article-footnote-368-40) discusses the nature of digital production and digital economy, the political economy of the key resources in the digital economy – data and digital intelligence derived from data, the public sector’s legitimate role in the new landscape, and lists important areas for engagement by public sector workers. Furthermore, according to longstanding international law, states have the sovereign right to safeguard and control the exploitation of their natural resources in the interest of citizens.

**1.12 Equitable application of labor laws for online work**

It is obvious that many types of work are moving online, either partly or entirely, and certain types of traditional work (such as taxi driving) are being transformed by online platforms.[41](https://projects.itforchange.net/digital-new-deal/2020/10/30/a-new-convention-for-data-and-cyberspace/#article-footnote-368-41) There is general agreement that labor laws must continue to be applied even as the economy transitions to more online work.[42](https://projects.itforchange.net/digital-new-deal/2020/10/30/a-new-convention-for-data-and-cyberspace/#article-footnote-368-42)

**1.13 Equitable application of consumer protection laws for online transactions**

In most countries, consumers have recourse to a fast and inexpensive national dispute resolution mechanism if they are dissatisfied with a product or service. But they rarely have effective recourse if the product or service was bought from a foreign vendor through the internet.[43](https://projects.itforchange.net/digital-new-deal/2020/10/30/a-new-convention-for-data-and-cyberspace/#article-footnote-368-43)

**1.14 Equitable distribution of the value of intellectual property rights**

Current intellectual property laws are dysfunctional and do not achieve their stated goals.[44](https://projects.itforchange.net/digital-new-deal/2020/10/30/a-new-convention-for-data-and-cyberspace/#article-footnote-368-44)

**1.15 Efficacy and safety of new technologies such as artificial intelligence**

More and more aspects of daily life are being controlled by automated devices, and in the near future, such devices will take over many services that are today provided manually, such as transportation. To do that, automated devices will have to make choices and decisions.[45](https://projects.itforchange.net/digital-new-deal/2020/10/30/a-new-convention-for-data-and-cyberspace/#article-footnote-368-45) It is important to ensure that these choices and decisions comply with our ethical values. In this context, it is worrisome that some modern artificial intelligence algorithms cannot be understood, to the point where it might be impossible to find out why an automated car malfunctioned.[46](https://projects.itforchange.net/digital-new-deal/2020/10/30/a-new-convention-for-data-and-cyberspace/#article-footnote-368-46)

At present, some actions have been proposed at the national level,[47](https://projects.itforchange.net/digital-new-deal/2020/10/30/a-new-convention-for-data-and-cyberspace/#article-footnote-368-47) but there does not appear to be adequate consideration of these issues at the international level.

As the above discussion shows, in certain key domains, current international law is not sufficiently explicit, meaning it does not map, with sufficient clarity, offline law to the online world. Based on these observations, the following section will explain why a new treaty is needed and how it could be negotiated.

**2. The need for a new treaty**

It has long been understood (and formalized in modern times in the 1648 Treaty of Westphalia) that there are, or should be, international rules restricting and/or guiding the ways in which states interact with themselves and with their citizens. Such rules are referred to as international law. The scope and density of international law has increased steadily over time, leading to fundamental advances such as the abolition of slavery and colonialism, the explicit formulation of fundamental human rights, and the formation of international agencies dedicated to the development of international law.

There are numerous treaties (the main source of international law) that relate to the rights and obligations of states regarding ICTs.[48](https://projects.itforchange.net/digital-new-deal/2020/10/30/a-new-convention-for-data-and-cyberspace/#article-footnote-368-48) However, as noted above, there are areas in which current international law is inadequate.

This gap has recently been explicitly recognized by most developed and some developing countries, which have joined together in the context of trade negotiations to develop treaty provisions that address some of the issues outlined above.[49](https://projects.itforchange.net/digital-new-deal/2020/10/30/a-new-convention-for-data-and-cyberspace/#article-footnote-368-49) However, the proposals that are being put forward are largely intended to enshrine the current situation, which favors dominant internet companies.[50](https://projects.itforchange.net/digital-new-deal/2020/10/30/a-new-convention-for-data-and-cyberspace/#article-footnote-368-50)

Several states too are initiating national processes that address some of the key issues outlined above. In that light, it would appear that states would be willing to support the initiation of a process to negotiate a new international treaty, specifically to address these matters. Such a treaty should not be an outcome of trade-related negotiations, because these issues are not directly linked to trade, and because trade negotiations are conducted in secret and without sufficient input from civil society and citizens.

It is likely that certain hegemonic powers (the US in particular) would oppose the negotiation of a new treaty along the lines outlined below. However, civil society and enlightened states could come together to negotiate a treaty without the US, as they have done in the past for banning nuclear weapons and certain types of conventional weapons, protection of geographic origin of products, etc. Once there is broad agreement on the content of a new treaty, its formalization would not necessarily be a long-drawn-out affair, as existing treaty-making mechanisms could be deployed to this end. In particular, the Plenipotentiary Conference held every four years – the next one will be in 2022 – by the International Telecommunication Union (ITU), could convene a World Conference on International Telecommunications (WCIT; the last one was held in 2012). WCIT could address many of the issues outlined above. Issues that are outside the scope of the ITU could be addressed in other forums such as ILO, UNCITRAL, UNCTAD, WIPO, etc.

Such a new treaty – a Convention for Data and Cyberspace – should be inspired by the Delhi Declaration[51](https://projects.itforchange.net/digital-new-deal/2020/10/30/a-new-convention-for-data-and-cyberspace/#article-footnote-368-51) and by the Digital Justice Manifesto.[52](https://projects.itforchange.net/digital-new-deal/2020/10/30/a-new-convention-for-data-and-cyberspace/#article-footnote-368-52)

**3. The contents of the new treaty**

The proposed new treaty would contain provisions along the following lines.[53](https://projects.itforchange.net/digital-new-deal/2020/10/30/a-new-convention-for-data-and-cyberspace/#article-footnote-368-53)

**3.1 Human rights**

* Parties shall adopt a binding instrument specifying that any restrictions to freedom of speech, freedom of communication, or privacy, on grounds of security concerns or otherwise, must be for strictly defined purposes and in accordance with globally accepted principles of necessity, proportionality, and judicial oversight. (See for example specific proposals by the JustNet Coalition.)[54](https://projects.itforchange.net/digital-new-deal/2020/10/30/a-new-convention-for-data-and-cyberspace/#article-footnote-368-54)

**3.2 Data**

* In order to ensure the protection of personal data, thus increasing consumer trust, Parties shall accede to Convention 108 of the Council of Europe and the 2018 protocol amending that convention (CM(2018)2 of May 18, 2018).
* Parties shall ensure that national laws regarding personal data conform to the provisions of Convention 108 as amended in 2018, and shall apply those provisions to cross-border data flows.
* Parties shall enact a national data policy which includes, in addition to personal data protection, provisions to ensure equitable distribution of the value derived from the monetization of data.

**3.3 Competition**

* Parties shall enact a national competition/antitrust law which is not restricted to preventing consumer harm.
* Parties shall develop and accede to global antitrust rules and an international enforcement mechanism for such rules.
* Parties shall enact data-sharing legislation.

**3.4 Taxation**

* Parties may impose local presence and/or data localization requirements in order to facilitate the enforcement of tax laws.
* Parties shall develop and accede to global taxation rules and an international enforcement mechanism for such rules.
* Parties may impose customs duties on data flows, in particular, when such flows are eroding existing tax bases and/or when alternate types of tax bases are insufficient to generate required tax revenues.

**3.5 Access to the internet**

* Parties shall accede to the 2012 version of the International Telecommunication Union’s *International Telecommunication Regulations*.
* Parties shall transpose to national law the provisions of ITU-Recommendation D.50, *International Internet Connection*.
* Each Party shall administer its procedures for the allocation and use of scarce telecommunications resources, including frequencies, telephone numbers, internet protocol addresses, internet domain names, and rights-of-way, in an objective, timely, transparent, and non-discriminatory manner, in public interest.

**3.6 Micro, small, and medium enterprises (MSMEs)**

* Parties shall ensure that MSMEs have affordable access to internet connectivity, international payment platforms, and international physical delivery services.
* Parties shall establish an international clearing house to facilitate and simplify mutual recognition of national e-signatures on customs and other legally required signed documents.
* Each Party shall ensure that retail platforms do not themselves supply goods or services offered for sale on the platform.

**3.7 Artificial intelligence**

* Parties shall adopt a model law or a treaty on ethical principles for artificial intelligence.

**3.8 Access to technology**

* Each Party shall ensure that enterprises around the world have access to modern technology on affordable, objective, timely, transparent, and non-discriminatory terms.
* Parties are encouraged to procure open source software for government use.
* No provisions of trade-related agreements shall be construed as preventing the procurement of open source software for government or private use.
* Access to source code may be mandated under national law for specific purposes, such as verification of compliance with national laws and regulations (competition, taxation, safety, environment, etc.).

**3.9 Consumer protection**

* Parties shall enact national law or regulations mandating minimum security requirements for ICT devices, in particular, those interconnected to form the Internet of Things (IoT).
* Parties shall enact national law or regulations to prohibit unsolicited commercial emails (spam) and shall establish effective enforcement mechanisms, including at the international level.
* Parties shall transpose to national law the provisions of ITU-Recommendation E.157, *International Calling Party Number Delivery*, and shall have enacted national laws prohibiting the misuse of international telephone numbers (see ITU-Recommendation E.156, *Guidelines for ITU-T Action on Reported Misuse of E.164 Number Resources*).

**3.10 Employment and working conditions**

* Parties shall take appropriate measures to address the employment issues arising from e-commerce, including by implementing relevant recommendations of the International Labour Organization.

**3.11 Security**

* Parties shall refrain from hacking personal accounts or private data held by journalists and private citizens involved in electoral processes.
* Parties shall refrain from using ICTs to steal the intellectual property of private companies, including trade secrets or other confidential business information, and to provide competitive advantage to other companies or commercial sectors.
* Parties shall refrain from inserting or requiring “backdoors” in mass-market commercial technology products.
* Parties shall agree to a clear policy for acquiring, retaining, securing, using, and reporting of vulnerabilities that reflects a strong mandate to report them to vendors in mass-market products and services.
* Parties shall exercise restraint in developing cyber weapons and ensure that any that are developed are limited, precise, and not reusable; Parties shall also ensure that they maintain control of their weapons in a secure environment.
* Parties shall agree to limit proliferation of cyber weapons; governments shall endeavor not to distribute, or permit others to distribute, cyber weapons and to use intelligence, law enforcement, and financial sanctions tools against those who do.
* Parties shall limit engagement in cyber offensive operations to avoid creating mass damage to civilian infrastructure or facilities.
* Parties shall endeavor to assist private sector efforts to detect, contain, respond, and recover in the face of cyberattacks; in particular, they shall enable the core capabilities or mechanisms required for response and recovery, including Computer Emergency Response Teams (CERTs); intervening in private sector response and recovery would be akin to attacking medical personnel at military hospitals.
* Parties shall facilitate the establishment of an international cyberattack attribution organization to strengthen trust online.
* Parties shall, individually and in cooperation, develop and apply measures to increase stability and security of international telecommunication networks and in the use of ICTs in order to achieve effective use thereof and avoidance of technical harm thereto, as well as to maintain international peace and security, the harmonious development of ICTs, and to prevent ICT practices that may pose threats to international peace and security.[55](https://projects.itforchange.net/digital-new-deal/2020/10/30/a-new-convention-for-data-and-cyberspace/#article-footnote-368-55)
* In case of ICT incidents, Parties shall consider all relevant information, including the larger context of the event, the challenges of attribution in the ICT environment, and the nature and extent of the consequences.
* Parties shall not knowingly allow their territory to be used for internationally wrongful acts using ICTs.
* Parties shall consider how best to cooperate to exchange information, assist each other, prosecute terrorist and criminal use of ICTs, and implement other cooperative measures to address such threats.
* Parties shall not conduct or knowingly support ICT activity contrary to their obligations under international law, that intentionally damages critical infrastructure, or otherwise impairs the use and operation of critical infrastructure to provide services to the public.
* Parties shall take appropriate measures to protect their critical infrastructure from ICT threats, taking into account General Assembly Resolution 58/199 on the creation of a global culture of cybersecurity and the protection of critical information infrastructures, and other relevant resolutions.
* Parties shall respond to appropriate requests for assistance by another State whose critical infrastructure is subject to malicious ICT acts; they shall also respond to appropriate requests to mitigate malicious ICT activity aimed at the critical infrastructure of another State emanating from their territory, taking into account due regard for sovereignty.
* Parties shall take reasonable steps to ensure the integrity of the supply chain so that end users can have confidence in the security of ICT products; they shall prevent the proliferation of malicious ICT tools and techniques and the use of harmful hidden functions.
* Parties shall encourage responsible reporting of ICT vulnerabilities, and share associated information on available remedies to such vulnerabilities, to limit and possibly eliminate potential threats to ICTs and ICT-dependent infrastructure.
* Parties shall not conduct, or knowingly support, activity to harm the information systems of the authorized emergency response teams (sometimes known as computer emergency response teams or cybersecurity incident response teams) of another State; a Party shall not use authorized emergency response teams to engage in malicious international activity.

**Notes**

[1](https://projects.itforchange.net/digital-new-deal/2020/10/30/a-new-convention-for-data-and-cyberspace/#article-footnote-hook-368-1) Richard Hill (2016) Internet governance, multi-stakeholder models, and the IANA transition: shining example or dark side?, *Journal of Cyber Policy*, 1:2, 176-197, DOI: 10.1080/23738871.2016.1227866.

[2](https://projects.itforchange.net/digital-new-deal/2020/10/30/a-new-convention-for-data-and-cyberspace/#article-footnote-hook-368-2) Hill, R. (2015). ‘The True Stakes of Internet Governance’. *Transnational Institute*. <https://www.tni.org/files/download/03_tni_state-of-power-2015_the_true_stakes_of_internet_governance-1.pdf>.

[3](https://projects.itforchange.net/digital-new-deal/2020/10/30/a-new-convention-for-data-and-cyberspace/#article-footnote-hook-368-3) Hill, Richard (2014), “The Internet, its governance, and the multi-Stakeholder model”, Info, vol. 16. no. 2, March 2014, section 5.3.

[4](https://projects.itforchange.net/digital-new-deal/2020/10/30/a-new-convention-for-data-and-cyberspace/#article-footnote-hook-368-4) <https://twn.my/title2/resurgence/2014/287-288/cover07.htm>.

[5](https://projects.itforchange.net/digital-new-deal/2020/10/30/a-new-convention-for-data-and-cyberspace/#article-footnote-hook-368-5) Hill, Richard (2013), “Internet governance: the last gasp of colonialism, or imperialism by other means”, in Rolf H. Weber, Roxana Radu, and Jean-Marie Chenou (eds), The evolution of global Internet policy: new principles and forms of governance in the making?, Schulthess/Springer, section 2.

[6](https://projects.itforchange.net/digital-new-deal/2020/10/30/a-new-convention-for-data-and-cyberspace/#article-footnote-hook-368-6) A/HRC/38/L.10/Rev.1, <https://documents-dds-ny.un.org/doc/UNDOC/LTD/G18/203/73/PDF/G1820373.pdf?OpenElement>.

[7](https://projects.itforchange.net/digital-new-deal/2020/10/30/a-new-convention-for-data-and-cyberspace/#article-footnote-hook-368-7) Nothias, Toussaint (2020), “Access granted: Facebook’s free basics in Africa”, *Media, Culture & Society*, Vol. 42(3) 329–348 <https://journals.sagepub.com/doi/full/10.1177/0163443719890530>.

[8](https://projects.itforchange.net/digital-new-deal/2020/10/30/a-new-convention-for-data-and-cyberspace/#article-footnote-hook-368-8) A/HRC/38/L.10/Rev.1, *op. cit.*

[9](https://projects.itforchange.net/digital-new-deal/2020/10/30/a-new-convention-for-data-and-cyberspace/#article-footnote-hook-368-9) A/HRC/38/L.10/Rev.1, *op. cit.*

[10](https://projects.itforchange.net/digital-new-deal/2020/10/30/a-new-convention-for-data-and-cyberspace/#article-footnote-hook-368-10) See in this respect the 30 March 2017 Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, document A/HRC/35/22. At  
<http://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/35/22>.

[11](https://projects.itforchange.net/digital-new-deal/2020/10/30/a-new-convention-for-data-and-cyberspace/#article-footnote-hook-368-11) See for example <https://www.theguardian.com/technology/2016/sep/09/facebook-deletes-norway-pms-post-napalm-girl-post-row>.

[12](https://projects.itforchange.net/digital-new-deal/2020/10/30/a-new-convention-for-data-and-cyberspace/#article-footnote-hook-368-12) <https://botpopuli.net/trump-and-cda-section-230-the-end-of-an-internet-exception>.

[13](https://projects.itforchange.net/digital-new-deal/2020/10/30/a-new-convention-for-data-and-cyberspace/#article-footnote-hook-368-13) A/HRC/38/L.10/Rev.1, *op. cit.*

[14](https://projects.itforchange.net/digital-new-deal/2020/10/30/a-new-convention-for-data-and-cyberspace/#article-footnote-hook-368-14) A/HRC/38/L.10/Rev.1, *op. cit.*

[15](https://projects.itforchange.net/digital-new-deal/2020/10/30/a-new-convention-for-data-and-cyberspace/#article-footnote-hook-368-15) JNC (2014), <http://justnetcoalition.org/2014/on_UN_HCHR_privacy_report.pdf>.

[16](https://projects.itforchange.net/digital-new-deal/2020/10/30/a-new-convention-for-data-and-cyberspace/#article-footnote-hook-368-16) A/RES/68/167, <https://undocs.org/A/RES/68/167>.

[17](https://projects.itforchange.net/digital-new-deal/2020/10/30/a-new-convention-for-data-and-cyberspace/#article-footnote-hook-368-17) A/RES/68/167, *op. cit.*

[18](https://projects.itforchange.net/digital-new-deal/2020/10/30/a-new-convention-for-data-and-cyberspace/#article-footnote-hook-368-18) <https://www.publicaffairsbooks.com/titles/shoshana-zuboff/the-age-of-surveillance-capitalism/9781610395694/>, <https://news.harvard.edu/gazette/story/2019/03/harvard-professor-says-surveillance-capitalism-is-undermining-democracy/>.

[19](https://projects.itforchange.net/digital-new-deal/2020/10/30/a-new-convention-for-data-and-cyberspace/#article-footnote-hook-368-19) <https://www.cigionline.org/publications/data-dangerous-comparing-risks-united-states-canada-and-germany-see-data-troves>.

[20](https://projects.itforchange.net/digital-new-deal/2020/10/30/a-new-convention-for-data-and-cyberspace/#article-footnote-hook-368-20) JNC (2014), *op. cit.*

[21](https://projects.itforchange.net/digital-new-deal/2020/10/30/a-new-convention-for-data-and-cyberspace/#article-footnote-hook-368-21) <https://www.schneier.com/blog/archives/2007/01/information_sec_1.html>; a comprehensive discussion is given in pages 103-107 of the Global Internet Report 2016 of the Internet Society, see in particular the examples on p. 101. The Report is available at: <https://www.internetsociety.org/globalinternetreport/2016/>. See also item 5 on page 8 of: <https://www.ntia.doc.gov/files/ntia/publications/eo_13800_botnet_report_for_public_comment.pdf>.

[22](https://projects.itforchange.net/digital-new-deal/2020/10/30/a-new-convention-for-data-and-cyberspace/#article-footnote-hook-368-22) ISOC (2016) <https://future.internetsociety.org/2016/index.html>.

[23](https://projects.itforchange.net/digital-new-deal/2020/10/30/a-new-convention-for-data-and-cyberspace/#article-footnote-hook-368-23) Indeed, there have been calls for such minimum standards. See for example sections 2.1 and 2.3 of <https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/infineon-nxp-st-enisa-position-on-cybersecurity>; pages 109 ff. of the Legislative Proposals of the US Cyberspace Solarium Committee, available at: <https://www.solarium.gov/>; and pages 15-21 of the “Cybersecurity Lessons from the Pandemic: Legislative Proposals”, same web site.

[24](https://projects.itforchange.net/digital-new-deal/2020/10/30/a-new-convention-for-data-and-cyberspace/#article-footnote-hook-368-24) <https://www.technologyreview.com/s/607954/why-tesla-is-worth-more-than-gm/> and  
<https://www.technologyreview.com/s/608095/it-pays-to-be-smart/>.

[25](https://projects.itforchange.net/digital-new-deal/2020/10/30/a-new-convention-for-data-and-cyberspace/#article-footnote-hook-368-25) Which is in fact the case for many dominant providers of services on the Internet, see:<https://www.technologyreview.com/s/607954/why-tesla-is-worth-more-than-gm/> and <https://www.technologyreview.com/s/608095/it-pays-to-be-smart/>; see also pages 9 and 12 of UNCTAD’s *Information Economy Report 2017: Digitalization, Trade and Development*, <http://unctad.org/en/pages/PublicationWebflyer.aspx?publicationid=1872>.

[26](https://projects.itforchange.net/digital-new-deal/2020/10/30/a-new-convention-for-data-and-cyberspace/#article-footnote-hook-368-26) <https://newint.org/features/2016/07/01/smiley-faced-monopolists/>; and the more radical criticism at: <http://www.rosalux-nyc.org/wp-content/files_mf/scholz_platformcoop_5.9.2016.pdf>; specific criticism of a dominant online retailer is at: <http://www.truth-out.org/news/item/38807-1-of-every-2-spent-online-goes-to-amazon-can-we-break-the-company-s-stranglehold> and <https://ilsr.org/amazon-stranglehold/>; see also: <http://www.nytimes.com/2016/12/13/opinion/forget-att-the-real-monopolies-are-google-and-facebook.html?_r=0>; and: <https://www.theguardian.com/commentisfree/2017/feb/19/the-observer-view-on-mark-zuckerberg>, and <https://www.theatlantic.com/technology/archive/2018/01/facebook-doesnt-care/551684/>. For a survey indicating that users are concerned about this issue, see: <https://ec.europa.eu/futurium/en/system/files/ged/ec_ngi_final_report_1.pdf>. For a very cogent historical analysis, making an analogy to the age of the Robber Barons, see: <http://www.potaroo.net/ispcol/2017-03/gilding.html>. See also pp. 18-19 of the World Bank’s 2016 Word Development Report (WDR-2016), titled “Digital Dividends”, available at: <http://documents.worldbank.org/curated/en/896971468194972881/pdf/102725-PUB-Replacement-PUBLIC.pdf>.

[27](https://projects.itforchange.net/digital-new-deal/2020/10/30/a-new-convention-for-data-and-cyberspace/#article-footnote-hook-368-27) <https://www.theguardian.com/technology/2017/jun/04/surge-pricing-comes-to-the-supermarket-dynamic-personal-data>

[28](https://projects.itforchange.net/digital-new-deal/2020/10/30/a-new-convention-for-data-and-cyberspace/#article-footnote-hook-368-28) <https://techcrunch.com/2016/11/28/ubers-china-app-is-now-separate-from-its-global-app-and-a-nightmare-for-foreigners/>.

[29](https://projects.itforchange.net/digital-new-deal/2020/10/30/a-new-convention-for-data-and-cyberspace/#article-footnote-hook-368-29) <http://www.huffingtonpost.com/entry/google-monopoly-barry-lynn_us_59a738fde4b010ca289a1155?section=us_politics> and <https://www.nakedcapitalism.com/2017/08/new-america-foundation-head-anne-marie-slaughter-botches-laundering-googles-money.html>.

[30](https://projects.itforchange.net/digital-new-deal/2020/10/30/a-new-convention-for-data-and-cyberspace/#article-footnote-hook-368-30) The European Commission found that Google had done this, see: <http://europa.eu/rapid/press-release_STATEMENT-17-1806_en.htm> and <http://europa.eu/rapid/press-release_MEMO-17-1785_en.htm>.

[31](https://projects.itforchange.net/digital-new-deal/2020/10/30/a-new-convention-for-data-and-cyberspace/#article-footnote-hook-368-31) <https://www.accc.gov.au/publications/digital-platforms-inquiry-final-report>.

[32](https://projects.itforchange.net/digital-new-deal/2020/10/30/a-new-convention-for-data-and-cyberspace/#article-footnote-hook-368-32) <http://www.boundary2.org/2018/10/richard-hill-too-big-to-be-review-of-wu-the-curse-of-bigness-antitrust-in-the-new-gilded-age/>.

[33](https://projects.itforchange.net/digital-new-deal/2020/10/30/a-new-convention-for-data-and-cyberspace/#article-footnote-hook-368-33) <https://unctad.org/en/pages/PublicationWebflyer.aspx?publicationid=2622>.

[34](https://projects.itforchange.net/digital-new-deal/2020/10/30/a-new-convention-for-data-and-cyberspace/#article-footnote-hook-368-34) <https://arstechnica.com/information-technology/2017/04/nsa-leaking-shadow-brokers-just-dumped-its-most-damaging-release-yet/>; <https://www.silicon.co.uk/security/nsa-malware-security-210253>; <https://www.vice.com/en_us/article/7x5vnz/notpetya-ushered-in-a-new-era-of-malware>.

[35](https://projects.itforchange.net/digital-new-deal/2020/10/30/a-new-convention-for-data-and-cyberspace/#article-footnote-hook-368-35) <https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/#sm.00017arazqit2faipqq2lyngzmxx4>.

[36](https://projects.itforchange.net/digital-new-deal/2020/10/30/a-new-convention-for-data-and-cyberspace/#article-footnote-hook-368-36) <http://www.oecd-ilibrary.org/taxation/addressing-the-tax-challenges-of-the-digital-economy_9789264218789-en>.

[37](https://projects.itforchange.net/digital-new-deal/2020/10/30/a-new-convention-for-data-and-cyberspace/#article-footnote-hook-368-37) See for example pp. vii and 2 of the GCIG report, available at: <https://www.cigionline.org/publications/one-internet>. Henceforth referenced as “GCIG”. See also 7.4 of  
<http://www.oecd-ilibrary.org/taxation/addressing-the-tax-challenges-of-the-digital-economy_9789264218789-en>; and <http://www.other-news.info/2016/12/they-have-right-now-another-you/>; and the study of data brokers at: <https://www.opensocietyfoundations.org/sites/default/files/data-brokers-in-an-open-society-20161121.pdf>; <https://www.internetsociety.org/blog/public-policy/2017/03/my-data-your-business>; <http://www.economist.com/news/leaders/21721656-data-economy-demands-new-approach-antitrust-rules-worlds-most-valuable-resource>; and <http://www.itu.int/en/council/cwg-internet/Pages/display-June2017.aspx?ListItemID=7>; and <https://www.theguardian.com/world/2017/aug/23/silicon-valley-big-data-extraction-amazon-whole-foods-facebook> and pages 6-7 of UNCTAD’s *Information Economy Report 2017: Digitalization, Trade and Development*, <http://unctad.org/en/pages/PublicationWebflyer.aspx?publicationid=1872> and <http://www.autoritedelaconcurrence.fr/doc/reportcompetitionlawanddatafinal.pdf> and <https://www.diplomacy.edu/blog/2018predictions#1>. An excellent discussion of this topic, with numerous references, is given in pp. 9 ff. of Third World Network, Briefing no. 3 for the World Trade Organization 11th Ministerial Conference, Buenos Aires, 10-13 December 2017, at: <http://www.twn.my/MC11/briefings/BP3.pdf>.

[38](https://projects.itforchange.net/digital-new-deal/2020/10/30/a-new-convention-for-data-and-cyberspace/#article-footnote-hook-368-38) <http://www.theatlantic.com/technology/archive/2014/08/advertising-is-the-internets-original-sin/376041/> and 7.4 of the cited OECD report; and <http://www.other-news.info/2016/12/they-have-right-now-another-you/> and  
<https://www.internetsociety.org/blog/public-policy/2017/03/my-data-your-business>.

[39](https://projects.itforchange.net/digital-new-deal/2020/10/30/a-new-convention-for-data-and-cyberspace/#article-footnote-hook-368-39) <https://unctad.org/en/pages/PublicationWebflyer.aspx?publicationid=2466>.

[40](https://projects.itforchange.net/digital-new-deal/2020/10/30/a-new-convention-for-data-and-cyberspace/#article-footnote-hook-368-40) [library.fes.de/pdf-files/iez/16034.pdf](http://library.fes.de/pdf-files/iez/16034.pdf).

[41](https://projects.itforchange.net/digital-new-deal/2020/10/30/a-new-convention-for-data-and-cyberspace/#article-footnote-hook-368-41) <https://repositorio.cepal.org/handle/11362/42046>.

[42](https://projects.itforchange.net/digital-new-deal/2020/10/30/a-new-convention-for-data-and-cyberspace/#article-footnote-hook-368-42) [https://www.ilo.org/global/topics/future-of-work/lang–en/index.htm](https://www.ilo.org/global/topics/future-of-work/lang--en/index.htm).

[43](https://projects.itforchange.net/digital-new-deal/2020/10/30/a-new-convention-for-data-and-cyberspace/#article-footnote-hook-368-43) <https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Consumer-Protection-Laws.aspx>.

[44](https://projects.itforchange.net/digital-new-deal/2020/10/30/a-new-convention-for-data-and-cyberspace/#article-footnote-hook-368-44) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3119041>; <https://www.theguardian.com/commentisfree/2012/nov/30/america-dysfunctional-patent-system-innovation>.

[45](https://projects.itforchange.net/digital-new-deal/2020/10/30/a-new-convention-for-data-and-cyberspace/#article-footnote-hook-368-45) <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML%2BCOMPARL%2BPE-582.443%2B01%2BDOC%2BPDF%2BV0//EN>.

[46](https://projects.itforchange.net/digital-new-deal/2020/10/30/a-new-convention-for-data-and-cyberspace/#article-footnote-hook-368-46) <https://www.technologyreview.com/s/604087/the-dark-secret-at-the-heart-of-ai/>.

[47](https://projects.itforchange.net/digital-new-deal/2020/10/30/a-new-convention-for-data-and-cyberspace/#article-footnote-hook-368-47) <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML%2BCOMPARL%2BPE-582.443%2B01%2BDOC%2BPDF%2BV0//EN> and <http://wam.ae/en/details/1395302639203>.

[48](https://projects.itforchange.net/digital-new-deal/2020/10/30/a-new-convention-for-data-and-cyberspace/#article-footnote-hook-368-48) <http://www.apig.ch/UNIGE%20Catalog.pdf>.

[49](https://projects.itforchange.net/digital-new-deal/2020/10/30/a-new-convention-for-data-and-cyberspace/#article-footnote-hook-368-49) <http://trade.ec.europa.eu/doclib/press/index.cfm?id=1974>.

[50](https://projects.itforchange.net/digital-new-deal/2020/10/30/a-new-convention-for-data-and-cyberspace/#article-footnote-hook-368-50) <https://ourworldisnotforsale.net/2017/ALAI_E-commerce.pdf>; <https://www.buzzfeednews.com/article/burcukilic/big-tech-is-pushing-for-a-new-kind-of-free-trade>; <https://ourworldisnotforsale.net/2019/WTO_12_reasons_v2.pdf>; additional references can be found at: <http://ourworldisnotforsale.net/>.

[51](https://projects.itforchange.net/digital-new-deal/2020/10/30/a-new-convention-for-data-and-cyberspace/#article-footnote-hook-368-51) <https://justnetcoalition.org/delhi-declaration>.

[52](https://projects.itforchange.net/digital-new-deal/2020/10/30/a-new-convention-for-data-and-cyberspace/#article-footnote-hook-368-52) <https://justnetcoalition.org/digital-justice-manifesto>.

[53](https://projects.itforchange.net/digital-new-deal/2020/10/30/a-new-convention-for-data-and-cyberspace/#article-footnote-hook-368-53) Detailed rationales for 3.2 through 3.10 are provided in [additional references](http://www.apig.ch/Development%20proposals.pdf).

[54](https://projects.itforchange.net/digital-new-deal/2020/10/30/a-new-convention-for-data-and-cyberspace/#article-footnote-hook-368-54) <http://justnetcoalition.org/2014/on_UN_HCHR_privacy_report.pdf>.

[55](https://projects.itforchange.net/digital-new-deal/2020/10/30/a-new-convention-for-data-and-cyberspace/#article-footnote-hook-368-55) This and the following provisions are based on the eleven norms of paragraph 13 of the 2015 Report of the UN Intergovernmental Group of Experts in the Field of Information and Telecommunications in the Context of International Security (UN document A/70/174), and on the 2012 International Telecommunication Regulations.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. <https://www.itu.int/md/S23-CL-C-0121/en> [↑](#footnote-ref-1)