|  |  |
| --- | --- |
|  | **Document EG-ITRs-3/2** |
| **10 July 2024** |
| **English only** |
|  |  |
| Contribution from HILL |
| Overall considerations and detailed analysis |
| **Purpose**This contribution discusses new trends in international Telecommunications/ICTs services relevant to be considered for the review of the ITRs; empirical data on the current use of the ITRs; and the relevance of the ITRs. This is in line with 2 of the ToR of the EG-ITRs. The first paragraph of each Annex of this contribution indicates the specific item (2(a), 2(b), 2(c)) of the ToR to which it is primarily related.**Action required**The Expert Group on the International Telecommunication Regulations is invited to **consider** this document.**References***Council* [*Resolution 1379*](https://www.itu.int/md/S23-CL-C-0121/en) *(Terms of Reference)* [*EG-ITRs-1/2*](https://www.itu.int/md/S23-EGITRS1-C-0002/en)*;* [*EG-ITRs-2/5*](https://www.itu.int/md/S24-EGITRS2-C-0005/en)*;* [*EG-ITRs-2/12*](https://www.itu.int/md/S24-EGITRS2-C-0012/en)*;* [*EG-ITRs 2/18*](https://www.itu.int/md/S24-EGITRS2-C-0018/en)*;* [*EG-ITRs-2/21*](https://www.itu.int/md/S24-EGITRS2-C-0021/en) |

This contribution is a revised version of [EG-ITRs-1/2](https://www.itu.int/md/S23-EGITRS1-C-0002/en), whose substance was not discussed in previous meetings; it is resubmitted as agreed at the second meeting (see 8.1 of [EG-ITRs-2/21](https://www.itu.int/md/S24-EGITRS2-C-0021/en)). The addendums to [EG-ITRs-1/2](https://www.itu.int/md/S23-EGITRS1-C-0002/en)have been incorporated as Annexes to this contribution.

**Summary**

It is appropriate to continue discussions on the ITRs. All international telecommunication services rely on the ITRs to some extent. The 2012 ITRs include provisions on new issues, for which binding treaty-level provisions have been proposed in trade negotiations. The use of AI in international telecommunication services should be discussed in the context of the ITRs, as this is a new trend/emerging issue. Some criticism of the 2012 ITRs is not justified. There are overlaps between ITU’s work and proposals made in trade negotiations.

Proposals made in trade negotiations indicate that agreement on treaty-level provisions regarding certain matters within the scope of ITU is a new trend and/or and emerging issue in telecommunications/ICTs and its environment which may impact the ITRs. In particular, there are provisions (agreed or proposed) in trade agreements regarding spam and cybersecurity.

In light of the above, Member States are invited to consider the situation and to consider how to address it in the context of the review of the ITRs. In particular, they may wish to consider: (a) Provisions should refer to, and bind, only Member States, not private parties. (Some of the language of the 1988 ITRs, which were agreed when there were still many state-owned monopoly telecommunications operators, was carried over to the 2012 ITRs.); (b) The ITRs should complement the CS/CV, not overlap with it; consequently, Member States may wish to consider abrogating, either in the CS/CV, or in the ITRs, provisions that overlap or are duplicative or redundant. (c) Member States may wish to consider whether new provisions are required to fill gaps and to address new/emerging issues.

A more detailed discussion for each of the articles of the 2012 ITRs, and for possible gap-filling, is provided in the annexes to this contribution.

**Proposal**

**1. Introduction**

1.1 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.

1.2 As shown below:

1. It is appropriate to continue discussions on the ITRs
2. All international telecommunication services rely on the ITRs to some extent
3. The 2012 ITRs include provisions on new issues, for which binding treaty-level provisions have been proposed in trade negotiations
4. The use of AI in international telecommunication services should be discussed in the context of the ITRs, as this is a new trend/emerging issue
5. Some criticism of the 2012 ITRs is not justified
6. There are overlaps between ITU’s work and proposals made in trade negotiations

1.3 Proposals made in trade negotiations indicate that agreement on treaty-level provisions regarding certain matters within the scope of ITU is a new trend and/or and emerging issue in telecommunications/ICTs and its environment which may impact the ITRs. In particular, there are provisions (agreed or proposed) in trade agreements regarding spam (see 1.16 below), cybersecurity (see 1.17 below), frequency allocation, and even network neutrality.

1.4 In light of the above, Member States are invited to consider the situation and to consider how to address it in the context of the review of the ITRs. In particular, they may wish to consider:

1. Provisions should refer to, and bind, only Member States, not private parties. (Some of the language of the 1988 ITRs, which were agreed when there were still many state-owned monopoly telecommunications operators, was carried over to the 2012 ITRs.)
2. The ITRs should complement the CS/CV, not overlap with it. Consequently, Member States may wish to consider abrogating, either in the CS/CV, or in the ITRs, provisions that overlap or are duplicative or redundant.
3. Member States may wish to consider whether new provisions are required to fill gaps and to address new/emerging issues.

1.5 A more detailed discussion for each of the articles of the 2012 ITRs, and for possible gap-filling, is provided in the Annexes to this contribution.

**1.1 It is appropriate to continue discussions on the ITRs**

1.6 As a preliminary matter, we note that absence of agreement is not an argument to stop discussions. On the contrary, absence of agreement indicates the necessity to continue discussions: interests and positions can change over time, as can technologies and policies.

1.7 Thus, in our view, it is appropriate to continue discussions on the ITRs until such time as consensus is reached.

**1.2 All international telecommunication services rely on the ITRs to some extent**

1.8 Further, contrary to what seems to be implied in some contributions to Council (C 73[[2]](#footnote-2), and C 66[[3]](#footnote-3)), all international telecommunication services rely on the ITRs to some extent, and the provisions of the ITRs **are** applicable in fostering the provision and development of international telecommunication/ICT services and networks. While most international telecommunication services no longer use the accounting rates of Article 6 of the 1988 ITRs, Internet traffic is enabled by the Special Arrangements of Article 9 of the 1988 ITRs[[4]](#footnote-4). Indeed, the 2012 ITRs recognize the fact, in their Article 8, that accounting rates are no longer prevalent, however Special Provisions were retained as Article 13, in order to ensure that Internet traffic would not be disrupted. See also the discussion regarding Articles 8 and 13 in the Annexes to this contribution.

1.9 Requests for empirical data on the current use of the ITRs by operating agencies will inevitably result in replies to the effect that the ITRs are not used by operating agencies, because, in the current environment, operating agencies are mostly private companies and thus not directly bound by the ITRs, which are a treaty. While some provisions of the ITRs might be transposed to national law, operating agencies have no reason to know that they are indirectly affected by the ITRs. See also 1.32(a) below.

1.10 Requests for empirical data on the current use of the ITRs by administrations and the proportion of global telecommunication services which now rely on the ITRs should result in replies to the effect that essentially all international Internet traffic is enabled by the Special Arrangements provision of the ITRs.

1.11 If today’s telecommunications services do not rely on the ITRs, and if the ITRs are no longer applicable, then why haven’t countries that are not signatories to the 2012 ITRs withdrawn from the 1988 ITRs, or suspended the operation of the 1988 ITRs, or proposed to terminate the ITRs[[5]](#footnote-5)? Surely if the ITRs are not needed, then Member States should withdraw from it, or propose to terminate it, instead of continuing to be bound by it.

**1.3 The 2012 ITRs include provisions on new issues, for which binding treaty-level provisions have been proposed in trade negotiations**

1.12 Further, the 2012 ITRs include provisions on new issues, in particular countering spam, security, e-waste, and accessibility. Many countries, including in particular developed countries, have proposed to negotiate binding treaty-level provisions for some of those issues in other forums, such as trade negotiations, see 1.23 ff. below and the Annexes to this contribution regarding the corresponding articles of the 2012 ITRs. Thus discussions on those issues should take place, regardless of whether or not certain provisions of the 1988 ITRs are no longer relied upon.

1.13 In particular, proposals being discussed in the WTO JSI, under the heading “D.2(2), Cooperation”, could be seen as an attempt to put the WTO in charge of every significant ICT issue, which means putting the WTO in charge of everything. Again, this underscores that discussions on those issues should take place, regardless of whether or not certain provisions of the 1988 ITRs are no longer relied upon.

1.14 And proposals being discussed in the WTO JSI, under the heading “D.3 Capacity building”, could be seen as an attempt to recreate ITU-D within WTO. This too underscores that discussions on those issues should take place, regardless of whether or not certain provisions of the 1988 ITRs are no longer relied upon.

1.15 The WTO JSI provisions on spam and security are far more detailed and prescriptive than the provision in the 2012 ITRs, see Annexes 6 and 7 to the present contribution.

1.16 The WTO JSI provision on spam includes a footnote that would appear to allow spam to be sent to an IP address; this could result in unwanted messages being sent directly to a user’s personal computer or smartphone, by targeting their IP address. For example, unwanted advertising could be sent directly to a personal computer or smartphone. Perhaps this was intended, in order to enshrine in a binding international treaty the current Internet funding model based on targeted advertising. Or perhaps it was not intended, and is a reflection of possible lack of technical knowledge by WTO negotiators.

1.17 Regarding security, one of the topics under discussion in the WTO JSI was whether to refer to “cybersecurity” – which has traditionally been used to refer to the non-content related technical aspects of ICT security, such as confidentiality and authentication – or to “information security” – which has traditionally been used within the United Nations to refer also to content-related aspects of ICT security, such as combating so-called disinformation.

1.18 Once again, the scope and nature of discussions in the WTO JSI indicates that discussions on spam and security should take place, regardless of whether or not certain provisions of the 1988 ITRs are no longer relied upon.

**1.4 The use of AI in international telecommunication services should be discussed in the context of the ITRs**

1.19 In addition, the emergence of Artificial Intelligence (AI) and software based upon it is a new trend and an emerging issue. While many aspects of AI are outside the scope of the ITU, surely the use of AI in international telecommunication services is squarely within the scope of the ITU. For example, AI can be used for network management, including traffic shaping (optimization of traffic). A committee of the US Congress has recently voted to request that a study be conducted on accountability measures for AI systems used by communications networks.[[6]](#footnote-6) As set forth in EG-ITRs-2/5:

6. Indeed, a good summary[[7]](#footnote-7) of recent governmental actions around the world regarding AI use and its regulation identifies the above as among the themes that have emerged in those actions. The learned author of that summary concludes:

Some will compare the emerging AI policy movement to the emergence of policy machinery a century ago for automobiles or broadcasting, each of which spawned the creation of thousands of regulatory agencies and rules worldwide. Regardless, the global policy community will now need to make room for a new AI regulation function, whether or not it’s ready.

7. We note in this context that, in October 2023, the UN Secretary-General convened a High-Level Advisory Body on Artificial Intelligence[[8]](#footnote-8). The Body’s immediate tasks include building a global scientific consensus on risks and challenges, helping harness AI for the Sustainable Development Goals, and strengthening international cooperation on AI governance.

8. And that, on 30 October 2023, the G7 Summit adopted the Hiroshima Process International Guiding Principles for Organizations Developing Advanced AI System[[9]](#footnote-9).

9. And that, also on 30 October 2023, the President of the United States of America issued an Executive Order directing actions that include[[10]](#footnote-10) “Promote the safe, responsible, and rights-affirming development and deployment of AI abroad to solve global challenges, such as advancing sustainable development and mitigating dangers to critical infrastructure.” Indeed section 11 (d) of the Executive Order[[11]](#footnote-11) states:

To address cross-border and global AI risks to critical infrastructure, the Secretary of Homeland Security, in coordination with the Secretary of State, and in consultation with the heads of other relevant agencies as the Secretary of Homeland Security deems appropriate, shall lead efforts with international allies and partners to enhance cooperation to prevent, respond to, and recover from potential critical infrastructure disruptions resulting from incorporation of AI into critical infrastructure systems or malicious use of AI.

10. Recent events regarding the Open AI organization reinforce the need for action. It appears that a dominant software company has, in effect, gained control of Open AI[[12]](#footnote-12). That company’s operating system is widely used, including in computers that provide critical infrastructure, including in the international telecommunication network. If AI is embedded in that operating system, without regulators or operating agencies being aware of the specifics of the embedded AI, then the AI could have unintended effects. For example, the AI could decide to cut off communications, on the grounds that it contributes to global warming, which must be avoided; or on the grounds that disinformation contributes to political unrest, which must be avoided.

11. A well respected and well known security expert has recently called for the regulation of AI, stating[[13]](#footnote-13): “We need AI transparency laws. When it is used. How it is trained. What biases and tendencies it has. We need laws regulating AI—and robotic—safety. When it is permitted to affect the world.”

12. The Council of Europe is developing a Framework Convention on Artificial Intelligence, Human Rights, Democracy and the Rule of Law public[[14]](#footnote-14). This indicates that a large number of developing countries believe that there is a need for treaty-level instruments to regulate certain aspects of AI.

13. Finally, and perhaps most importantly, the European Union has reached an agreement on harmonized binding rules on artificial intelligence (AI), the so-called artificial intelligence act[[15]](#footnote-15). According to this Regulation[[16]](#footnote-16), AI systems intended to be used as safety components in the management and operation of critical digital infrastructure are considered “high-risk AI systems” (see Annex III, 2(a) of the Regulation). Key provisions regarding high-risk AI systems can be summarized as follows:

1. high-risk AI systems are subject to certain requirements with respect to training data (Art. 10 of the Regulation),
2. high-risk AI systems must be transparent (Art. 13 of the Regulation),
3. high-risk AI systems must be subject to human oversight (Art. 14 of the Regulation), and
4. providers and users of high-risk AI systems must ensure compliance with the provisions of the Regulation (Arts. 16-21 and 29 of the Regulation).

14. If AI systems can affect the safety of the management or operation of the international telecommunication network (which is obviously a critical digital infrastructure), then they are subject to the provisions of the cited European Union Regulation.

1.20 In March 2024, the UN General Assembly unanimously adopted Resolution A/78/L.49[[17]](#footnote-17), initially proposed by the United States, and subsequently co-sponsored by 120 states, on AI[[18]](#footnote-18). That Resolution states, inter alia:

Encourages Member States and invites multi-stakeholders from all regions and countries, within their respective roles and responsibilities, including …, international and regional organizations, … to develop and support regulatory and governance approaches and frameworks related to safe, secure and trustworthy artificial intelligence systems … recognizing that effective partnership and cooperation between Governments and multi-stakeholders is necessary in developing such approaches and frameworks;

1.21 In May 2024, the US State of Colorado enacted a law on AI that is similar to the European Union’s regulation mentioned in 1.19.13 above[[19]](#footnote-19).

1.22 Thus there appears to be an emerging consensus[[20]](#footnote-20) that, at a minimum:

1. AI systems should be transparent: it should be clear when something is AI-produced, and the training data and model architectures should be disclosed;
2. builders of AI systems should be made accountable for the outputs produced;
3. AI systems should not have full autonomous control of critical systems or infrastructure (which would include basic telecommunications infrastructure).

1.23 Specific suggestions regarding AI are given in Annex 3 to this contribution.

**1.5 Some criticism of the 2012 ITRs is not justified**

1.24 Criticism of the 2012 ITRs has been addressed in academic writings[[21]](#footnote-21), [[22]](#footnote-22), which show that some of that criticism is not justified from a legal point of view.

**1.6 There are overlaps between ITU’s work and proposals made in trade negotiations**

1.25 There are numerous overlaps between work carried out in the International Telecommunication Union (ITU) and trade-related proposals regarding e-commerce and telecommunications that have been agreed in plurilateral instrument such at the Trans-Pacific Partnership (TPP)[[23]](#footnote-23) or that are being proposed for discussion in the context of the World Trade Organization (WTO) work on e-commerce[[24]](#footnote-24) or other plurilateral agreements such as Trade in Services (TISA).

1.26 Indeed, several Member States, in particular developed countries, have proposed, in the WTO Joint Statement Initiative (JSI) on e-commerce, that provisions regarding matters covered by the 2012 ITRs should be agreed and somehow made binding for at least some WTO members.

1.27 We refer here, and include by reference, the analysis in sections 2 through 11 of EG-ITRs-1/02 regarding this matter.

1.28 As shown there, many of the provisions go against what has been agreed in ITU. It is not clear why trade negotiations should be used to override agreements made in a specialized agency that has greater expertise in the subject matter than does an agency whose mandate is to facilitate international trade.

1.29 Further, in some cases developed countries have made proposals in free trade negotiations that are exactly the opposite of the proposals that they have made in ITU. For example, developed countries have opposed detailed binding provisions on international mobile roaming in ITU, but agreed them in TPP (and proposed them in TISA and plurilateral agreements such as the JSI on e-commerce); the same holds for a provision on recourse to national authorities by foreign enterprises; and for provisions on security and for countering spam.[[25]](#footnote-25) And, more recently, proposals have been made in the JIS on e-commerce with respect to network neutrality, whereas developed countries have opposed including such provisions in the ITRs.

**1.7 Conclusion**

1.30 In light of the above, it appears that agreement on treaty-level provisions regarding those matters is a new trend and/or and emerging issue in telecommunications/ICTs.

1.31 This has led to comments from civil society[[26]](#footnote-26), [[27]](#footnote-27), [[28]](#footnote-28).

1.32 The trends/emerging issues in question may impact the ITRs.

1.33 Further, since new provisions are being proposed/agreed, it appears that additional high-level guiding principles for in the current telecommunication/ICT environment should be introduced in the ITRs.

1.34 Therefore, Member States are invited to consider the situation and to consider how to address it in the context of the review of the ITRs. In particular, they may wish to consider:

1. Provisions should refer to, and bind, only Member States, not private parties. (Some of the language of the 1988 ITRs, which were agreed when there were still many state-owned monopoly telecommunications operators, was carried over to the 2012 ITRs.)
2. The ITRs should complement the CS/CV, not overlap with it. Consequently, Member States may wish to consider abrogating, either in the CS/CV, or in the ITRs, provisions that overlap or are duplicative or redundant.
3. Member States may wish to consider whether new provisions are required to fill gaps and to address new/emerging issues.

1.35 A more detailed discussion for each of the articles of the 2012 ITRs, and for possible gap-filling to address new trends and emerging issues, is provided in the Annexes to this contribution.

**Annex 1
Preamble and Art. 1: Purpose and Scope**

1. This annex focuses on the Preamble and Art. 1 of the 2012 ITRs, Purpose and Scope. It relates primarily to 2(c) of the ToR of the EG-ITRs.

2. They state:

**Preamble**

While the sovereign right of each State to regulate its telecommunications is fully recognized, the provisions of the present International Telecommu-nication Regulations (hereafter referred to as “Regulations”) supplement complement the Constitution and the Convention of the International Telecommunication Union, with a view to attaining the purposes of the International Telecommunication Union in promoting the development of telecommunication services and their most efficient operation while harmonizing the development of facilities for worldwide telecommunications.

Member States affirm their commitment to implement these Regulations in a manner that respects and upholds their human rights obligations.

These Regulations recognize the right of access of Member States to inter-national telecommunication services.

**Article 1: Purpose and Scope of the Regulations**

1.1 *a)* These Regulations establish general principles which relate to the provision and operation of international telecommunication services offered to the public as well as to the underlying international telecommunication transport means used to provide such services. These Regulations do not address the content-related aspects of telecommunications.

*b)* These Regulations also contain provisions applicable to those operating agencies, authorized or recognized by a Member State, to establish, operate and engage in international telecommunications services to the public, hereinafter referred as "authorized operating agencies".

 *c)* These Regulations recognize in Article 13 the right of Member States to allow special arrangements.

1.2 In these Regulations, “the public” is used in the sense of the population, including governmental and legal bodies.

1.3 These Regulations are established with a view to facilitating global interconnection and interoperability of telecommunication facilities and to promoting the harmonious development and efficient operation of technical facilities, as well as the efficiency, usefulness and availability to the public of international telecommunication services.

1.4 References to Recommendations of the ITU Telecommunication Standardization Sector (ITU-T) in these Regulations are not to be taken as giving to those Recommendations the same legal status as these Regulations.

1.5 Within the framework of these Regulations, the provision and operation of international telecommunication services in each relation is pursuant to mutual agreement between authorized operating agencies.

1.6 In implementing the principles of these Regulations, authorized operating agencies should comply with, to the greatest extent practicable, the relevant ITU-T Recommendations.

1.7 *a)* These Regulations recognize the right of any Member State, subject to national law and should it decide to do so, to require that authorized operating agencies which operate in its territory and provide an international telecommunication service to the public be authorized by that Member State.

 *b)* The Member State concerned shall, as appropriate, encourage the application of relevant ITU-T Recommendations by such service providers.

 *c)* The Member States, where appropriate, shall cooperate in implementing these Regulations.

1.8 These Regulations shall apply, regardless of the means of transmission used, so far as the Radio Regulations do not provide otherwise.

**Discussion of Preamble**

3. As noted in an academic writing[[29]](#footnote-29), the first two paragraphs of the Preamble are not problematic, while the third paragraph has no operative effect (because it is in a preamble).

4. Therefore, Member States are invited to consider the situation and to consider how to address it in the context of the review of the ITRs, for example by considering whether to abrogate the third paragraph.

**Discussion of Purpose and Scope**

5. Criticism of the Purpose and Scope has been addressed in academic writings [[30]](#footnote-30), [[31]](#footnote-31).

6. Since the ITRs are a treaty, its provisions should refer only to obligations and rights of Member States. They should not purport to have direct effects on private sector entities. If a state wishes to impose certain obligations on private sector entities within its jurisdiction, it can do so through national laws and/or regulations, in accordance with their sovereign rights and article 1.7(a) of the 2012 ITRs.

7. Therefore, Member States are invited to consider the situation and to consider how to address it in the context of the review of the ITRs, for example by considering whether to abrogate articles 1.1(b) and 1.6 of the 2012 ITRs, and consequently removing all references to “operating agencies” from the rest of the ITRs.

**Annex 2
Art. 2: Definitions**

1. This Annex focuses on Art. 2 of the 2012 ITRs, Definitions. It relates primarily to 2(c) of the ToR of the EG-ITRs.

2. It states:

2.1 For the purpose of these Regulations, the following definitions shall apply. These terms and definitions do not, however, necessarily apply for other purposes.

2.2 *Telecommunication:* Any transmission, emission or reception of signs, signals, writing, images and sounds or intelligence of any nature by wire, radio, optical or other electromagnetic systems.

2.3 *International telecommunication service:* The offering of a telecommunication capability between telecommunication offices or stations of any nature that are in or belong to different countries.

2.4 *Government telecommunications:* Telecommunications originating with any: Head of State; Head of a government or members of a government; Commanders-in-Chief of military forces, land, sea or air; diplomatic or consular agents; the Secretary-General of the United Nations; Heads of the principal organs of the United Nations; the International Court of Justice, or replies to government telecommunications mentioned above.

2.5 *Service telecommunication:* A telecommunication that relates to public international telecommunications and that is exchanged among the following:

– Member States;

– authorized operating agencies; and

– the Chairman of the Council, the Secretary-General, the Deputy Secretary-General, the Directors of the Bureaux, the members of the Radio Regulations Board, and other representatives or authorized officials of the Union, including those working on official matters outside the seat of the Union.

2.6 *International route:* Technical facilities and installations located in different countries and used for telecommunication traffic between two international telecommunication terminal exchanges or offices.

2.7 *Relation:* Exchange of traffic between two terminal countries, always referring to a specific service, if there is between their authorized operating agencies:

*a)* a means for the exchange of traffic in that specific service:

– over direct circuits (direct relation), or

– via a point of transit in a third country (indirect relation), and

*b)* normally, the settlement of accounts.

2.8 *Accounting rate:* The rate agreed between authorized operating agencies, in a given relation that is used for the establishment of international accounts.

2.9 *Collection charge:* The charge established and collected by an authorized operating agency from its customers for the use of an international telecommunication service.

**Discussion of Definitions**

3. As noted in an academic writing[[32]](#footnote-32), the first four definitions (arts. 2.2-2.5) overlap with the ITU Constitution (the same terms are defined in the same way).

4. In our view, the other definitions (2.6-2.9) are longer no relevant (see discussion regarding Article 8).

5. Therefore, Member States are invited to consider the situation and to consider how to address it in the context of the review of the ITRs, for example by considering whether to abrogate this article.

**Annex 3
Art. 3: International Network**

1. This Annex focuses on Art. 3 of the 2012 ITRs, International Network. It relates primarily to 2(a) and 2(c) of the ToR of the EG-ITRs.

2. It states:

3.1 Member States shall endeavour to ensure that authorized operating agencies cooperate in the establishment, operation and maintenance of the international network to provide a satisfactory quality of service.

3.2 Member States shall endeavour to ensure the provision of sufficient telecommunication facilities to meet the demand for international telecommunication services.

3.3 Authorized operating agencies shall determine by mutual agreement which international routes are to be used. Pending agreement and provided that there is no direct route existing between the terminal authorized operating agencies concerned, the origin authorized operating agency has the choice to determine the routing of its outgoing telecommunication traffic, taking into account the interests of the relevant transit and destination authorized operating agencies.

3.4 Subject to national law, any user, by having access to the international network, has the right to send traffic. A satisfactory quality of service should be maintained to the greatest extent practicable, corresponding to the relevant ITU-T Recommendations.

3.5 Member States shall endeavour to ensure that international telecommunication numbering resources specified in ITU-T Recommendations are used only by the assignees and only for the purposes for which they were assigned; and that unassigned resources are not used.

3.6 Member States shall endeavour to ensure that international calling line identification (CLI) information is provided taking into account the relevant ITU-T Recommendations.

3.7Member States should create an enabling environment for the implementation of regional telecommunication traffic exchange points, with a view to improving quality, increasing the connectivity and resilience of networks, fostering competition and reducing the costs of international telecommunication interconnections.

**Discussion of Article 3**

2. In our view, article 3.3 is no longer relevant, nor should it be included in the ITRs, because it purports to impose obligations directly on private sector entities (see the discussion regarding article 1 of the ITRs).

3. In our view, the remaining provisions remain valid and should not be changed.

4. Until recently, in Europe (and presumably elsewhere) calls to certain international numbers (in particular +882 and +883) could be made, even when those numbers are used for safety of life (in particular, eCall)[[33]](#footnote-33). This is an undesirable situation: national regulators should ensure that all ITU-assigned numbering resources can be used properly.

5. As noted in no. 1.19 ff. of the main contribution (“Overall considerations”), the emergence of Artificial Intelligence (AI) and software based upon it is a new trend and an emerging issue. While many aspects of AI are outside the scope of the ITU, surely the use of AI in international telecommunications services is squarely within the scope of the ITU. For example, AI can be used for network management, including traffic shaping (optimization of traffic). There appears to be an emerging consensus that some limits should be placed on the way AI systems are deployed.

6. In light of the above, Member States are invited to consider the situation and to consider how to address it in the context of the review of the ITRs, for example by considering whether to abrogate article 3.3 and whether to add new articles along the following lines:

1. Member States shall ensure, through national regulation, that all international numbering resources assigned and published by ITU can be dialed and are routed in their jurisdictions.
2. Member States shall endeavour to ensure that AI systems used for the international telecommunication network are transparent: it should be clear when something is AI-produced, and the training data and model architectures should be disclosed.
3. Member States shall ensure that builders of AI systems used for the international telecommunication network are accountable for the outputs produced.
4. Member States shall ensure that AI systems do not have full autonomous control of critical systems or infrastructure used for the international telecommunication network (which would include basic telecommunications infrastructure).

**Annex 4
Art. 4: International Telecommunication Services**

1. This Annex focuses on Art. 4 of the 2012 ITRs, International Telecommunication Services. It relates primarily to 2(c) of the ToR of the EG-ITRs.

2. It states:

4.1 Member States shall promote the development of international telecommunication services and shall foster their availability to the public.

4.2 Member States shall endeavour to ensure that authorized operating agencies cooperate within the framework of these Regulations to provide, by agreement, a wide range of international telecommunication services which should conform, to the greatest extent practicable, to the relevant ITU-T Recommendations.

4.3 Subject to national law, Member States shall endeavour to ensure that authorized operating agencies provide and maintain, to the greatest extent practicable, a satisfactory quality of service corresponding to the relevant ITU-T Recommendations with respect to:

*a)* access to the international network by users using terminals which are permitted to be connected to the network and which do not cause harm to technical facilities and personnel;

*b)* international telecommunication facilities and services available to users for their dedicated use;

*c)* at least a form of telecommunication service which is reasonably accessible to the public, including those who may not be subscribers to a specific telecommunication service; and

*d)* a capability for interworking between different services, as appropriate, to facilitate international telecommunication services.

4.4 Member States shall foster measures to ensure that authorized operating agencies provide free-of-charge, transparent, up-to-date and accurate information to end users on international telecommunication services, including international roaming prices and the associated relevant conditions, in a timely manner.

4.5 Member States shall foster measures to ensure that telecommunication services in international roaming of satisfactory quality are provided to visiting users.

4.6 Member States should foster cooperation among authorized operating agencies in order to avoid and mitigate inadvertent roaming charges in border zones.

4.7Member States shall endeavour to promote competition in the provision of international roaming services and are encouraged to develop policies that foster competitive roaming prices for the benefit of end users.

**Discussion of Article 4**

3. In our view, this article remains valid and should not be changed.

**Annex 5
Art. 5: Safety of life and priority of telecommunications**

1. This Annex focuses on Art. 5 of the 2012 ITRs, Safety of life and priority of telecommunications. It relates primarily to 2(c) of the ToR of the EG-ITRs.

2. It states:

5.1 Safety-of-life telecommunications, such as distress telecommunications, shall be entitled to transmission as of right and, where technically practicable, have absolute priority over all other telecommunications, in accordance with the relevant articles of the Constitution and the Convention and taking due account of the relevant ITU-T Recommendations.

5.2 Government telecommunications, including telecommunications relative to the application of certain provisions of the United Nations Charter, shall, where technically practicable, enjoy priority over telecommunications other than those referred to in No. 45 (5.1) above, in accordance with the relevant provisions of the Constitution and the Convention and taking due account of the relevant ITU-T Recommendations.

5.3 The provisions governing the priority enjoyed by *any* other telecommunication service are contained in the relevant ITU-T Recommendations.

5.4 Member States should encourage authorized operating agencies to inform all users, including roaming users, in good time and free of charge, of the number to be used for calls to the emergency services.

**Discussion of Article 5**

3. As stated in an academic writing [[34]](#footnote-34) this provision overlaps considerably with Articles 40 and 41 of the ITU Constitution.

4. Therefore, Member States are invited to consider the situation and to consider how to address it in the context of the review of the ITRs: Member States could consider either abrogating the respective portions of Articles 40 and 41 of the ITU Constitution, or abrogating this article of the ITRs.

**Annex 6
Art. 6: Security and robustness of networks**

1. This Annex focuses on art. 6 of the 2012 ITRs, Security and robustness of networks. It relates primarily to 2(a), 2(b), and 2(c) of the ToR of the EG-ITRs.

2. It states:

6.1 Member States shall individually and collectively endeavor to ensure the security and robustness of international telecommunication networks in order to achieve effective use thereof and avoidance of technical harm thereto, as well as the harmonious development of international telecommunication services offered to the public.

**Discussion of Article 6**

3. Criticism of this provision has been addressed in academic writings[[35]](#footnote-35), [[36]](#footnote-36).

4. Starting in 2017, several Member States, in particular developed countries, proposed that provisions regarding cybersecurity should be included in free trade agreements, including those agreed in the World Trade Organization (WTO).

5. Indeed, Security experts have long recognized that the lack of information and communication technology (ICT) security creates a negative externality.[[37]](#footnote-37) 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.[[38]](#footnote-38)

6. 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?[[39]](#footnote-39)

7. As stated in 2017 by the Microsoft president[[40]](#footnote-40):

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.

8. On 21 February 2024, the following text was submitted for discussion in the WTO, by the Joint Statement Initiative (JSI) on e-commerce [[41]](#footnote-41):

Article 23: Cybersecurity

1. The Parties recognize that threats to cybersecurity undermine confidence in digital trade.

2. The Parties recognize the evolving nature of cyber threats. In order to identify and mitigate those threats and thereby facilitate electronic commerce the Parties shall endeavor to:

 (a) build the capabilities of their respective nation entities responsible for cybersecurity incident response; and

(b) collaborate to identify and mitigate malicious intrusions or dissemination of malicious code that affect electronic networks of Parties and to address cybersecurity incidents in a timely manner, as well as to share information for awareness and best practices.

3. Given the evolving nature of cyber threats and their negative impact on electronic commerce, the Parties recognize the importance of risk-based approaches in addressing those threats while minimizing trade barriers. Accordingly, each [Party/Member] shall endeavor to employ, and to encourage enterprises within its jurisdiction to use, risk-based approaches that rely on risk management best practices and on standards developed in a consensus-based, transparent, and open manner, to identify and protect against cybersecurity risks, to detect cybersecurity events, and to respond to and recover from cybersecurity incidents.

9. As can be seen, the provision being discussed in the WTO JSI in 2022 is far more detailed and prescriptive than the provision in the 2012 ITRs. (From the legislative history, it appears that the reference to “standards developed in a consensus-based, transparent, and open manner” is a reference to “Principles for the Development of International Standards, Guides and Recommendations”:
 <https://www.wto.org/english/tratop_e/tbt_e/principles_standards_tbt_e.htm> )

10. Thus it appears that many Member States, in particular developed countries, are of the view that binding treaty-level provisions regarding cybersecurity are needed, and that they should be more detailed than the generic provision found in the 2012 ITRs.

11. Indeed, in September 2022, the European Commission published a proposal for a regulation on cybersecurity requirements for products with digital elements, known as the Cyber Resilience Act, whose intent is to bolster cybersecurity rules to ensure more secure hardware and software products.[[42]](#footnote-42)

12. It is worth noting that one of the topics under discussion in the WTO JSI was whether to refer to “cybersecurity” – which has traditionally been used to refer to the non-content related technical aspects of ICT security, such as confidentiality and authentication – or to “information security” – which has traditionally been used within the United Nations to refer also to content-related aspects of ICT security, such as combating so-called disinformation[[43]](#footnote-43). We note that the final proposal referred to “cybersecurity”.

13. Consequently, it appears that agreement on treaty-level provisions regarding cybersecurity is a new trend and/or and emerging issue in telecommunications/ICTs and its environment. (This has lead to comments from civil society[[44]](#footnote-44), [[45]](#footnote-45), [[46]](#footnote-46).)

14. Further, since new provisions are being proposed/agreed, it appears that the provisions of the 2012 ITRs do not provide appropriate high-level guiding principles in the current telecommunication/ICT environment.

15. Therefore, Member States are invited to consider the situation and to consider how to address it in the context of the review of the ITRs. In particular, Member States may wish to consider the following possible commitments[[47]](#footnote-47):

1. Parties shall refrain from hacking personal accounts or private data held by journalists and private citizens involved in electoral processes.
2. 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.
3. Parties shall refrain from inserting or requiring “backdoors” in mass-market commercial technology products.
4. 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.
5. 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.
6. 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.
7. Parties shall limit engagement in cyber offensive operations to avoid creating mass damage to civilian infrastructure or facilities.
8. 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.
9. Parties shall facilitate the establishment of an international cyberattack attribution organization to strengthen trust online.
10. 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.[[48]](#footnote-48)
11. 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.
12. Parties shall not knowingly allow their territory to be used for internationally wrongful acts using ICTs.
13. 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.
14. 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.
15. 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.
16. 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.
17. 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.
18. 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.
19. 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.

**Annex 7
Art. 7: Unsolicited bulk electronic communications**

1. This Annex focuses on Art. 7 of the 2012 ITRs, Unsolicited bulk electronic communications. It relates primarily to 2(a), 2(b), and 2(c) of the ToR of the EG-ITRs.

2. It states:

7.1 Member States should endeavor to take necessary measures to prevent the propagation of unsolicited bulk electronic communications and minimize its impact on international telecommunication services.

7.2 Member States are encouraged to cooperate in that sense.

**Discussion of Article 7**

3. Criticism of this provision has been addressed in academic writings[[49]](#footnote-49), [[50]](#footnote-50).

4. Starting in 2017, several Member States, in particular developed countries, proposed that provisions regarding spam should be included in free trade agreements, including those agreed in the World Trade Organization (WTO).

5. On 21 February 2024, the following text was submitted for discussion in the WTO, by the Joint Statement Initiative (JSI) on e-commerce [[51]](#footnote-51):

Article 20: Unsolicited commercial electronic messages

20.1 For the purposes of this Article:

(a) "Commercial electronic message" means an electronic message which is sent for commercial purposes to an electronic address of a person {FN1} through telecommunication services, comprising at least electronic mail and to the extent provided for under domestic laws and regulations, other types of messages.

(b) "Unsolicited commercial electronic message" means a commercial electronic message that is sent without the consent of the recipient or despite the explicit rejection of the recipient.

20.2 Parties recognize the importance of promoting confidence and trust in electronic commerce, including through transparent and effective measures that limit unsolicited commercial electronic messages. Each Party shall adopt or maintain measures that:

(a) require suppliers of commercial electronic messages to facilitate the ability of recipients to prevent ongoing reception of those messages; or

(b) require the consent, as specified in the laws or regulations of each Party, of recipients to receive commercial electronic messages; or

(c) otherwise provide for the minimization of unsolicited commercial electronic messages.

20.3 Each Party shall endeavor to ensure that commercial electronic messages are clearly identifiable as such, clearly disclose on whose behalf they are sent, and contain the necessary information to enable recipients to request cessation free of charge and at any time.

20.4 Each Party shall provide access to either redress or recourse against suppliers of unsolicited commercial electronic messages that do not comply with the measures adopted or maintained pursuant to paragraph 20.2.

20.5 Parties shall endeavor to cooperate in appropriate cases of mutual concern regarding the regulation of unsolicited commercial electronic messages.

{FN1}: For greater certainty, the “electronic address of a person” does not cover IP addresses.

6. As can be seen, the provision propose by the WTO JSI is far more detailed and prescriptive than the provision in the 2012 ITRs.

7. Thus it appears that many Member States, in particular developed countries, are of the view that binding treaty-level provisions to combat spam are needed, and that they should be more detailed than the generic provision found in the 2012 ITRs.

8. Consequently, it appears that agreement on treaty-level provisions to combat spam is a new trend and/or and emerging issue in telecommunications/ICTs and its environment. (This has lead to comments from civil society[[52]](#footnote-52), [[53]](#footnote-53), [[54]](#footnote-54).)

9. Further, since new provisions are being proposed/agreed, it appears that the provisions of the 2012 ITRs do not provide appropriate high-level guiding principles in the current telecommunication/ICT environment.

10. Therefore, Member States are invited to consider the situation and to consider how to address it in the context of the review of the ITRs.

11. We note in passing that the footnote {FN1} in the WTO provision would appear to allow spam to be sent to an IP address; this could result in unwanted messages being sent directly to a user’s personal computer or smartphone, by targeting their IP address. For example, unwanted advertising could be sent directly to a personal computer or smartphone. Perhaps this was intended, in order to enshrine in a binding international treaty the current Internet funding model based on targeted advertising. Or perhaps it was not intended, and is a reflection of possible lack of technical knowledge by WTO negotiators.

**Annex 8
Art. 8: Charging and accounting**

1. This Annex focuses on Art. 8 of the 2012 ITRs, Charging and accounting. It relates primarily to 2(a), 2(b), and 2(c) of the ToR of the EG-ITRs.

It states:

**8.1 International telecommunication arrangements**

8.1.1 Subject to applicable national law, the terms and conditions for international telecommunication service arrangements may be established through commercial agreements or through accounting-rate principles established pursuant to national regulation.

8.1.2 Member States shall endeavour to encourage investments in international telecommunication networks and promote competitive wholesale pricing for traffic carried on such telecommunication networks.

**8.2 Accounting-rate principles**

***Terms and conditions***

8.2.1 The following provisions may apply where the terms and conditions of international telecommunication service arrangements are established through accounting-rate principles, established pursuant to national regulation. These provisions do not apply to arrangements established through commercial agreements.

8.2.2 For each applicable service in a given relation, authorized operating agencies shall, by mutual agreement, establish and revise accounting rates to be applied between them, in accordance with the provisions of Appendix 1 and taking into account the relevant ITU-T Recommendations.

8.2.3 Unless otherwise agreed, parties engaged in the provision of international telecommunication services shall follow the relevant provisions as set out in Appendices 1 and 2.

8.2.4 In the absence of special arrangements concluded between authorized operating agencies, the monetary unit to be used in the composition of accounting rates for international telecommunication services and in the establishment of international accounts shall be:

– either the monetary unit of the International Monetary Fund (IMF), currently the Special Drawing Right (SDR), as defined by that organization;

– or freely convertible currencies or other monetary unit agreed between the authorized operating agencies.

***Collection charges***

8.2.5 The charges levied on customers for a particular communication should in principle be the same in a given relation, regardless of the international route used for that communication. In establishing these charges, Member States should try to avoid dissymmetry between the charges applicable in each direction of the same relation.

**8.3 Taxation**

8.3.1 Where, in accordance with the national law of a country, a fiscal tax is levied on collection charges for international telecommunication services, this tax shall normally be collected only in respect of international services billed to customers in that country, unless other arrangements are made to meet special circumstances.

**8.4 Service telecommunications**

8.4.1 Authorized operating agencies may in principle forgo the inclusion of service telecommunications in international accounting, under the relevant provisions of the Constitution and the Convention and these Regulations, having due regard for the need for reciprocal arrangements. Authorized operating agencies may provide service telecommunications free of charge.

8.4.2 The general operational, charging and accounting principles applicable to service telecommunications should take account of the relevant ITU-T Recommendations.

**Discussion of Article 8**

3. As stated in an academic writing [[55]](#footnote-55) article 8.1.1 does nothing other than to recognize the current reality: most telecommunication charging and accounting is negotiated by private sector entities, possibility with some conditions imposed by some national regulations (e.g. for roaming).

4. Since the provision is a mere statement of fact, and does not impose any rights or obligations on Member States, it does not, in our view, belong in a treaty.

5. Article 8.1.2 encourages states to take measures to encourage investments in telecommunications. In our view, this is a useful provision and it should remain unchanged.

6. The provisions under 8.2 (8.2.1-8.2.5) refer to accounting and charging methods that are used only in certain jurisdictions. Those jurisdictions can enshrine such methods in national law, or in regional agreements, if they so wish. In our view, these provisions are no longer useful.

7. Indeed, as stated in EG-ITRs-2/12, operators in developed countries no longer use the accounting rate system. The prevalence of charging and accounting by privately negotiated agreements is thus a new (compared to 1988) trend that has been recognized in 8.1.1 of the 2012 ITRs and that should be more explicitly recognized by abrogating 8.2.1-8.2.5 of the 2012 ITRs.

8. Further, there is an increasing impact of so-called over-the-top (OTT) services, see 6, 8, and 11 of EG-ITRs 2/18 and:

 <https://www.itu.int/en/ITU-T/studygroups/2013-2016/03/Pages/ott.aspx>

This is a new and emerging trend that warrants discussion, in particular regarding whether provisions regarding charging and accounting for OTTs should be considered for inclusion in the ITRs.

9. The provisions under 8.4 (8.4.1-8.4.2) do not create rights or obligations for Member States: they purport to apply to private sector entities. As such, in our view, they do not belong in the ITRs, see the discussion regarding Article 1, Purpose and Scope.

10. Article 8.3.1, on taxation, is notoriously difficult to understand, interpret, and apply. If there is a desire to specify something about double taxation, then it should be stated clearly. In our view, the current provision is not useful and does not provide appropriate high-level guiding principles in the current telecommunication/ICT environment. Indeed, as stated in 10 of EG-ITRs 2/18, the current provision may limit revenue collection for developing countries, impacting infrastructure development.

11. In light of the above, Member States are invited to consider the situation and to consider how to address it in the context of the review of the ITRs: Member States could consider abrogating all provisions of this article, except for 8.1.2, and, if desired, develop clear language regarding taxation to replace the current article 8.3.1, and/or new language regarding OTTs.

**Annex 9
Art. 9: Suspension of services**

1. This Annex focuses on Art. 9 of the 2012 ITRs, Suspension of services. It relates primarily to 2(c) of the ToR of the EG-ITRs.

2. It states:

9.1 If a Member State exercises its right in accordance with the Constitution and the Convention to suspend international telecommunication services partially or totally, that Member State shall immediately notify the Secretary-General of the suspension and of the subsequent return to normal conditions by the most appropriate means of communication.

9.2 The Secretary-General shall immediately bring such information to the attention of all other Member States, using the most appropriate means of communication.

**Discussion of Article 9**

3. As stated in an academic writing [[56]](#footnote-56) this provision overlaps considerably with Articles 1 (no. 18) and 35 of the ITU Constitution, and with Article 5 (nos. 98 and 99) of the ITU Convention.

4. Therefore, Member States are invited to consider the situation and to consider how to address it in the context of the review of the ITRs: Member States could consider either abrogating the respective portions of Articles 1 and 35 of the ITU Constitution and Article 5 of the ITU Constitution, or abrogating this article of the ITRs.

**Annex 10
Art. 10: Dissemination of information**

1. This Annex focuses on Art. 10 of the 2012 ITRs, Dissemination of information. It relates primarily to 2(c) of the ToR of the EG-ITRs.

2. It states:

10.1 Using the most suitable and economical means, the Secretary-General shall disseminate information provided, of an administrative, operational, tariff or statistical nature, concerning international telecommunication routes and services. Such information shall be disseminated in accordance with the relevant provisions of the Constitution and the Convention and of this Article, on the basis of decisions taken by the Council or by competent ITU conferences, and taking account of conclusions or decisions of ITU assemblies. If so authorized by the Member State concerned, the information may be transmitted to the Secretary-General directly by an authorized operating agency, and shall then be disseminated by the Secretary-General. Member States should transmit such information to the Secretary-General in a timely manner, taking into account the relevant ITU-T Recommendations.

**Discussion of Article 10**

3. In our view, this article remains valid and should not be changed.

**Annex 11
Art. 11: Energy efficiency/e-waste**

1. This Annex focuses on Art. 11 of the 2012 ITRs, Energy efficiency/e-waste. It relates primarily to 2(c) of the ToR of the EG-ITRs.

2. It states:

11.1 Member States are encouraged to adopt energy-efficiency and e-waste best practices taking into account the relevant ITU-T Recommendations.

**Discussion of Article 11**

3. In our view, this article remains valid and should not be changed, and this in particular because e-waste is rising five times faster than documented e-waste recycling, see:

 <https://www.itu.int/en/mediacentre/Pages/PR-2024-03-20-e-waste-recycling.aspx>

4. According to a joint ITU/UNITAR report (cited in the above reference):

* The 62 million tonnes of e-waste generated in 2022 would fill 1.55 million 40-tonne trucks, roughly enough trucks to form a bumper-to-bumper line encircling the equator.
* Meanwhile, less than one quarter (22.3 per cent) of the year's e-waste mass was documented as having been properly collected and recycled in 2022, leaving USD 62 billion worth of recoverable natural resources unaccounted for and increasing pollution risks to communities worldwide.
* Worldwide, the annual generation of e-waste is rising by 2.6 million tonnes annually, on track to reach 82 million tonnes by 2030, a further 33 per cent increase from the 2022 figure.

**Annex 12
Art. 12: Accessibility**

1. This Annex focuses on Art. 12 of the 2012 ITRs, Accessibility. It relates primarily to 2(c) of the ToR of the EG-ITRs.

2. It states:

12.1 Member States should promote access for persons with disabilities to international telecommunication services, taking into account the relevant ITU-T Recommendations.

**Discussion of Article 12**

3. In our view, this article remains valid and should not be changed.

**Annex 13
Art. 13: Special arrangements**

1. This Annex focuses on Art. 13 of the 2012 ITRs, Special Arrangements. It relates primarily to 2(c) of the ToR of the EG-ITRs.

2. It states:

13.1 *a)* Pursuant to Article 42 of the Constitution, special arrangements may be entered into on telecommunication matters which do not concern Member States in general. Subject to national laws, Member States may allow authorized operating agencies or other organizations or persons to enter into such special mutual arrangements with Member States and authorized operating agencies, or other organizations or persons that are so allowed in another country for the establishment, operation and use of special international telecommunication networks, systems and services, in order to meet specialized international telecommunication needs within and/or between the territories of the Member States concerned, and including, as necessary, the financial, technical or operating conditions to be observed .

 *b)* Any such special arrangements shall endeavour to avoid technical harm to the operation of the telecommunication facilities of third countries.

13.2 Member States should, where appropriate, encourage the parties to any special arrangements that are made pursuant to No. 73 (13.1) above to take into account relevant provisions of ITU-T Recommendations.

**Discussion of Article 13**

3. As stated in an academic writing [[57]](#footnote-57) this provision overlaps considerably with article 8.1.1 of the 2012 ITRs and with Article 42 of the ITU Constitution.

4. Therefore, Member States are invited to consider the situation and to consider how to address it in the context of the review of the ITRs: Member States could consider either abrogating Article 42 of the ITU Constitution, or revising it to conform to art. 13 of the 2012 ITRs and abrogating that article.

**Annex 14
Art. 14: Final provisions**

1. This Annex focuses on Art. 14 of the 2012 ITRs, the Final provisions. It relates primarily to 2(c) of the ToR of the EG-ITRs.

2. It states:

14.1 These Regulations, of which Appendices 1 and 2 form integral parts, shall enter into force on 1 January 2015, and shall be applied as of that date, consistent with all the provisions of Article 54 of the Constitution.

14.2 If a Member State makes reservations with regard to the application of one or more of the provisions of these Regulations, other Member States shall be free to disregard the said provision or provisions in their relations with the Member State which has made such reservations.

**Discussion of Article 14**

3. In our view, Appendix 1 is no longer relevant (see discussion regarding Article 8).

4. Therefore, Member States are invited to consider the situation and to consider how to address it in the context of the review of the ITRs, for example by considering whether to abrogate Appendix 1, and to revise Article 14 accordingly, including changing the dates to reflect the date of approval of a new version of the ITRs.

**Annex 15
New trends in telecommunications/ICT and emerging issues in international telecommunications/ICT environment which may impact the ITRs**

This Annex focuses on new trends in telecommunications/ICT and emerging issues in international telecommunications/ICT environment which may impact the ITRs. It relates primarily to 2(a) of the ToR of the EG-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 Annexes. 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/#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)
2. <https://www.itu.int/md/S23-CL-C-0073/en> [↑](#footnote-ref-2)
3. <https://www.itu.int/md/S23-CL-C-0066/en> [↑](#footnote-ref-3)
4. Hill, Richard (2013) *The New International Telecommunications Regulations and the Internet: A Commentary and Legislative History*,Schulthess/Springer, p. 8 [↑](#footnote-ref-4)
5. See Article 65 of the Vienna Convention on the Law of Treaties [↑](#footnote-ref-5)
6. <https://www.meritalk.com/articles/house-panel-takes-step-toward-ai-regulation/> [↑](#footnote-ref-6)
7. https://thehill.com/opinion/technology/4389011-making-sense-of-2023s-tsunami-of-ai-policy-changes/ [↑](#footnote-ref-7)
8. <https://www.un.org/techenvoy/ai-advisory-body> [↑](#footnote-ref-8)
9. <https://www.mofa.go.jp/files/100573471.pdf> [↑](#footnote-ref-9)
10. FACT SHEET: President Biden Issues Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence, available at:
<https://www.whitehouse.gov/briefing-room/statements-releases/2023/10/30/fact-sheet-president-biden-issues-executive-order-on-safe-secure-and-trustworthy-artificial-intelligence/> [↑](#footnote-ref-10)
11. <https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/> [↑](#footnote-ref-11)
12. <https://gizmodo.com/ai-safety-openai-sam-altman-ouster-back-microsoft-1851038439> [↑](#footnote-ref-12)
13. <https://www.belfercenter.org/publication/ai-and-trust> [↑](#footnote-ref-13)
14. <https://www.coe.int/en/web/artificial-intelligence/cai>
<https://www.coe.int/en/web/artificial-intelligence/home> [↑](#footnote-ref-14)
15. <https://www.consilium.europa.eu/en/press/press-releases/2023/12/09/artificial-intelligence-act-council-and-parliament-strike-a-deal-on-the-first-worldwide-rules-for-ai/> [↑](#footnote-ref-15)
16. <https://data.consilium.europa.eu/doc/document/ST-14954-2022-INIT/en/pdf> [↑](#footnote-ref-16)
17. <https://undocs.org/A/78/L.49> [↑](#footnote-ref-17)
18. <https://news.un.org/en/story/2024/03/1147831> [↑](#footnote-ref-18)
19. <https://insightplus.bakermckenzie.com/bm/data-technology/north-america-from-brussels-to-boulder-colorado-enacts-comprehensive-ai-law-on-the-heels-of-eus-ai-act-with-significant-obligations-for-business-and-employers> [↑](#footnote-ref-19)
20. The US government has obtained voluntary commitments from leading AI companies, see:

 <https://www.whitehouse.gov/briefing-room/statements-releases/2023/07/21/fact-sheet-biden-harris-administration-secures-voluntary-commitments-from-leading-artificial-intelligence-companies-to-manage-the-risks-posed-by-ai/> ; and it plans to internationalize those commitments, see:
 <https://insidetrade.com/daily-news/blinken-raimondo-promise-ai-coordination-democratic-partners> .

The European Parliament is developing a regulation, see:
 <https://www.europarl.europa.eu/news/en/press-room/20230505IPR84904/ai-act-a-step-closer-to-the-first-rules-on-artificial-intelligence> .

The US Congress may consider some measures, see:
 <https://www.foxnews.com/politics/house-baby-step-ai-regulation-government-accountability> .
For an AI developer’s point of view, see:
 <https://aiguide.substack.com/p/thoughts-on-a-crazy-week-in-ai-news> . [↑](#footnote-ref-20)
21. Hill, Richard (2013) ["WCIT: failure or success, impasse or way forward?"](http://ijlit.oxfordjournals.org/content/21/3/313.abstract), *International Journal of Law and Information Technology,* vol. 21 no. 3, p. 313,  DOI:10.1093/ijlit/eat008 [↑](#footnote-ref-21)
22. Hill, Richard (2013) *The New International Telecommunications Regulations and the Internet: A Commentary and Legislative History*,Schulthess/Springer, p. 75 [↑](#footnote-ref-22)
23. The full text of TPP is available at:
 <https://ustr.gov/trade-agreements/free-trade-agreements/trans-pacific-partnership/tpp-full-text> [↑](#footnote-ref-23)
24. The text being negotiated in WTO is not publicly available, but a recently leaked version can be found here:
 <https://www.bilaterals.org/?wto-2023-plurilateral-ecommerce-48862> [↑](#footnote-ref-24)
25. For more details see Hill, Richard (2013) *The New International Telecommunications Regulations and the Internet: A Commentary and Legislative History,* Schulthess/Springer [↑](#footnote-ref-25)
26. <https://www.newsclick.in/Why-Spam-Trade-Issue-Suits-Dominant-Developed-Countries> [↑](#footnote-ref-26)
27. <http://apig.ch/WTO%20ITU%20overlaps%20paper.pdf> [↑](#footnote-ref-27)
28. Hill, Richard (2020) “[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) [↑](#footnote-ref-28)
29. Hill, Richard (2013) *The New International Telecommunications Regulations and the Internet: A Commentary and Legislative History*,Schulthess/Springer, p. 86 [↑](#footnote-ref-29)
30. Hill, Richard (2013) ["WCIT: failure or success, impasse or way forward?"](http://ijlit.oxfordjournals.org/content/21/3/313.abstract), *International Journal of Law and Information Technology,* vol. 21 no. 3, p. 313,  DOI:10.1093/ijlit/eat008 [↑](#footnote-ref-30)
31. Hill, Richard (2013) *The New International Telecommunications Regulations and the Internet: A Commentary and Legislative History*,Schulthess/Springer, p. 87 [↑](#footnote-ref-31)
32. Hill, Richard (2013) *The New International Telecommunications Regulations and the Internet: A Commentary and Legislative History*,Schulthess/Springer, p. 93 [↑](#footnote-ref-32)
33. <https://eena.org/blog/resolving-the-ecall-callback-issue/> [↑](#footnote-ref-33)
34. Hill, Richard (2013) *The New International Telecommunications Regulations and the Internet: A Commentary and Legislative History*,Schulthess/Springer, p. 101 [↑](#footnote-ref-34)
35. Hill, Richard (2013) ["WCIT: failure or success, impasse or way forward?"](http://ijlit.oxfordjournals.org/content/21/3/313.abstract), *International Journal of Law and Information Technology,* vol. 21 no. 3, p. 313,  DOI:10.1093/ijlit/eat008 [↑](#footnote-ref-35)
36. Hill, Richard (2013) *The New International Telecommunications Regulations and the Internet: A Commentary and Legislative History*,Schulthess/Springer, p. 75 [↑](#footnote-ref-36)
37. <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>. [↑](#footnote-ref-37)
38. ISOC (2016) <https://future.internetsociety.org/2016/index.html>. [↑](#footnote-ref-38)
39. 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. [↑](#footnote-ref-39)
40. <https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/#sm.00017arazqit2faipqq2lyngzmxx4>. [↑](#footnote-ref-40)
41. WTO document INF/ECOM/85/Rev.1. The proponents include at least the 76 countries listed here: <https://www.wto.org/english/tratop_e/ecom_e/joint_statement_e.htm>
and likely the 86 listed here: <https://wtoplurilaterals.info/plural_initiative/e-commerce/> [↑](#footnote-ref-41)
42. <https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act> . A detailed commentary of this proposal can be found here: <https://berthub.eu/articles/posts/eu-cra-secure-coding-solution/> [↑](#footnote-ref-42)
43. See <https://disarmament.unoda.org/ict-security/> [↑](#footnote-ref-43)
44. <https://www.newsclick.in/Why-Spam-Trade-Issue-Suits-Dominant-Developed-Countries> [↑](#footnote-ref-44)
45. <http://apig.ch/WTO%20ITU%20overlaps%20paper.pdf> [↑](#footnote-ref-45)
46. Hill, Richard (2020) “[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) [↑](#footnote-ref-46)
47. Taken from 3.11 of:
 <https://projects.itforchange.net/digital-new-deal/2020/10/30/a-new-convention-for-data-and-cyberspace/> [↑](#footnote-ref-47)
48. 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 Regulation. [↑](#footnote-ref-48)
49. Hill, Richard (2013) ["WCIT: failure or success, impasse or way forward?"](http://ijlit.oxfordjournals.org/content/21/3/313.abstract), *International Journal of Law and Information Technology,* vol. 21 no. 3, p. 313,  DOI:10.1093/ijlit/eat008 [↑](#footnote-ref-49)
50. Hill, Richard (2013) *The New International Telecommunications Regulations and the Internet: A Commentary and Legislative History*,Schulthess/Springer, p. 75 [↑](#footnote-ref-50)
51. WTO document INF/ECOM/85/Rev.1. The proponents include at least the 76 countries listed here: <https://www.wto.org/english/tratop_e/ecom_e/joint_statement_e.htm>
and likely the 86 listed here: <https://wtoplurilaterals.info/plural_initiative/e-commerce/> [↑](#footnote-ref-51)
52. <https://www.newsclick.in/Why-Spam-Trade-Issue-Suits-Dominant-Developed-Countries> [↑](#footnote-ref-52)
53. <http://apig.ch/WTO%20ITU%20overlaps%20paper.pdf> [↑](#footnote-ref-53)
54. Hill, Richard (2020) “[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) [↑](#footnote-ref-54)
55. Hill, Richard (2013) *The New International Telecommunications Regulations and the Internet: A Commentary and Legislative History*,Schulthess/Springer, p. 104 [↑](#footnote-ref-55)
56. Hill, Richard (2013) *The New International Telecommunications Regulations and the Internet: A Commentary and Legislative History*,Schulthess/Springer, p. 109 [↑](#footnote-ref-56)
57. Hill, Richard (2013) *The New International Telecommunications Regulations and the Internet: A Commentary and Legislative History*,Schulthess/Springer, p. 112 [↑](#footnote-ref-57)