Contribution to the second meeting of the
Intergovernmental Group or Experts on E-commerce and the Digital Economy
February 2018
Richard Hill[1], APIG

Summary

The key barriers to e-commerce that need to be overcome are to reduce the cost of connectivity; to maintain trust and security, including by maintaining privacy and data protection rights; to address disruptive effects on jobs and income distribution; and to ensure that dominant players do not abuse their market power.

Reducing the cost of connectivity can be achieved by fostering competition (which may include functional separation), funding infrastructure, taking steps to reduce the cost of international connectivity, supporting the development of local content, capacity building, and a proper governance system.

Maintaining trust and security can be achieved by protecting human rights, protecting data privacy, combating spam, protecting consumers, enabling pervasive strong encryption, and curtailing unnecessary and disproportionate mass surveillance.

Further, it is time to recognize the time has come to make the world a better place by using the Internet to increase social justice: the fair and just relation between the individual and society, measured in terms of the explicit and tacit terms for the distribution of wealth, opportunities for personal activity and social privileges. And the time has come to abandon neo-liberal policies that are in reality corporatist policies that favor the techno-imperialistic goals of a few large companies.

Introduction

On 6 October 2017[2] the UNCTAD Intergovernmental Group of Experts on E-commerce and the Digital Economy decided[3] that its second session should focus on the following questions:

> (a) How can developing countries foster local platforms for domestic and cross-border e-commerce?
>
> (b) What are the existing barriers related to international e-commerce platforms that developing countries, including the least developed countries, face and how can these barriers be overcome?
>
> (c) What are some of the operational constraints that small and medium-sized businesses in developing countries face when setting up trade online, and how can they be overcome?
>
> (d) What are the good practices that developed and developing countries, including the least developed countries, can learn from each other?

In response to those questions, we first outline the key challenges facing developing countries and micro, small and medium enterprises (MSMEs) with respect to e-commerce and the digital economy, and then provide our comments regarding the specific questions above.

---

[1] info@apig.ch

[2] http://unctad.org/en/Pages/MeetingDetails.aspx?meetingid=1437

[3] http://unctad.org/meetings/en/SessionalDocuments/tdb_ede2017_agreedpolicyrecommendations_agenda2ndsession_en.pdf

1. Challenges

The challenges posed by e-commerce and the digital economy have been well summarized in the 26 July 2017 Note by the Secretariat titled "Maximizing the development gains from e-commerce and the digital economy", document TD/B/EDE/1/2[4] and the subsequent 14 February 2018 Note titled "Fostering development gains from e-commerce and digital platforms", document TD/B/EDE/2/2[5]. Several of the issues mentioned below are also well summarized in Chapter 4 of ITU, Measuring the Information Society Report 2017, Vol. 1[6].

As stated in paragraphs 13 and 15 of the cited July 2017 Note, and in paragraphs 8, 44 and 45-47 of the cited February 2018 Note, digital divides remain wide both across and within countries[7]. Thus a key issue that must be addressed is the lack of affordable access in many developing countries[8], and for disadvantaged groups in many countries.

It is important to recognize that most e-commerce is domestic (paragraphs 19-22 of the cited July 2017 Note and paragraph 7 of the cited February 2018 Note), so domestic policies are more important than international policies.

Issues related to the flow and processing of data, in particular in light of the development of interconnected devices (the Internet of Things – IoT), are increasingly important (paragraphs 27, 42, and 43 of the cited July 2017 Note). As paragraph 18 of the cited February 2018 Note correctly states: "Data have indeed become a valuable extractable resource in the digital economy."

Digital divides and uneven access to affordable connectivity can lead to inequitable income distribution and growing income inequality (paragraphs 38 and 41 of the cited July 2017 Note and 45-47 of the cited February 2018 Note).

There may be increasing concentration of market power and wealth (paragraph 41 of the cited July 2017 Note)[9], and disruptive effects on labour (paragraph 40 of the cited July 2017 Note).

UNCTAD makes similar points in its *Information Economy Report 2017: Digitalization, Trade and Development*[10]:[11]

> Digitalization will create opportunities for entrepreneurs and businesses, while also bringing enormous benefits to consumers. However, at the same time it will disrupt existing practices,

[4] http://unctad.org/meetings/en/SessionalDocuments/tdb_ede1d2_en.pdf

[5] http://unctad.org/meetings/en/SessionalDocuments/tdb_ede2d2_en.pdf

[6] https://www.itu.int/en/ITU-D/Statistics/Documents/publications/misr2017/MISR2017_Volume1.pdf

[7] See also pp. 12 and 16 of the 2017 report of the Broadband Commission, at: https://www.itu.int/dms_pub/itu-s/opb/pol/S-POL-BROADBAND.18-2017-PDF-E.pdf

[8] See pages 46 and 84 of UNCTAD's *Information Economy Report 2017: Digitalization, Trade and Development*, http://unctad.org/en/pages/PublicationWebflyer.aspx?publicationid=1872

[9] E-commerce is characterized by network effects that can lead to concentration, see p. 6 of the September 2017 International Trade Center (ITC) paper "New Pathways to E-Commerce: A Global MMSE Competitiveness Survey", CEES-17-105-E, available at: http://www.intracen.org/publication/New-Pathways-to-E-commerce/

[10] http://unctad.org/en/pages/PublicationWebflyer.aspx?publicationid=1872

[11] The citation is from p. iv.

> expose incumbents to competition, change skills requirements of workers and result in job losses in some countries and sectors.
>
> …
>
> Like previous large-scale economic transitions, the benefits will be immense, but they will not materialize through a smooth, cost-free process. The net outcome will depend on policies undertaken at both national and international levels to build countries' capabilities to take advantage of these transformations

Similar points are made in the Report of the 6-8 December 2016, Mexico City, UN Expert Group Meeting on Exponential Technological Change, Automation, and Their Policy Implications for Sustainable Development[12] ("exponential technologies" refers to technologies that exhibit exponential growth, including big data, artificial intelligence, the Internet, etc.). And in one expert's predictions for 2018[13] and in a recent book from a major ICT company[14] and an article by a well known Internet engineer[15].

These are not new thoughts. As a scholar put the matter back in 2002[16]:

> "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."

There is a lack of competition at the international level. As a scholar puts the matter: "when we look at what the digital economy has done over the past two decades, what becomes clear is that it has created an enormous amount of value for consumers and for a small group of big companies, even as it has diminished competition, centralised power, and made life much more difficult for businesses that

---

[12] https://sustainabledevelopment.un.org/content/documents/15295Meeting_report_final.pdf . Additional papers on achieving the Sustainable Development Goals are published at: https://sustainabledevelopment.un.org/index.php?menu=1027

[13] https://www.diplomacy.edu/blog/2018predictions

[14] https://blogs.microsoft.com/blog/2018/01/17/future-computed-artificial-intelligence-role-society/

[15] Andrew Sullivan, "Avoiding lamentation: to build a future Internet", *Journal of Cyberpolicy*, vol. 2, no. 3, pp. 323-337, available at: http://www.tandfonline.com/doi/full/10.1080/23738871.2017.1400083 . Regarding the dangers of one company dominating artificial intelligence, see: https://www.wired.com/story/google-artificial-intelligence-monopoly/

[16] Baird, Zoe (2002) "Governing the Internet: Engaging Government, Business, and Nonprofits", *Foreign Affairs*, vol. 81, no. 6, November/December 2002. Available at: http://www.markle.org/sites/default/files/06_baird_15_20_0.pdf

produce content or try to compete with the economy's dominant players."[17] The advent of the Internet has favored concentration and this has contributed to rising income inequality.[18]

As the Secretary-General of UNCTAD put the matter when introducing UNCTAD' Trade and Development Report 2017: "the world economy remains unbalanced in ways that are not only exclusionary, but also destabilizing and dangerous for the political, social and environmental health of the planet. Even when economic growth has been possible, whether through a domestic consumption binge, a housing boom or exports, the gains have disproportionately accrued to the privileged few."[19]

As a speaker put the matter at a meeting[20] of a working group of the UN Human Rights Council, referring to the work of the well known economist Joseph Stiglitz: "… globalization distinctly disadvantaged developing countries … Market failure and the dominant role of finance not only affected inequality between nations, but also within nations, including within advanced economies. … there is a growing trend to combat this."[21]

Companies in developing countries may not have adequate access to the e-commerce platforms used in developed countries, and/or the terms of access, including loss of control over data, may be unfavorable.[22] E-payment platforms may not be accessible or available in developing countries.[23] Cross-border delivery may be difficult for both companies and consumers in developing countries.[24] It may be difficult to comply with differing data protection laws across jurisdictions.[25]

There are increased security risks for entities that connect to the Internet, due to hacking, viruses, cyber-attacks, etc. (paragraph 44 of the cited July 2017 Note).

Further, fulfilment of the WTO's Doha Development Agenda mandate, such as on substantial reduction of OTDS in Agriculture; Cotton; and Special and Differential Treatment, with the view to promoting structural transformation and industrialization, would be of benefit to MSMEs in Africa.[26]

MSMEs are the least likely to be able to effectively compete with multinational corporations, who have become global digital leaders, and have decimated smaller companies and who have benefitted from

---

[17] https://www.technologyreview.com/s/607954/why-tesla-is-worth-more-than-gm/ ; see also the first paragraph of Wu, Tim, Antitrust Via Rulemaking: Competition Catalysts (October 24, 2017), *Colorado Technology Law Journal*, https://ssrn.com/abstract=3058114

[18] https://www.nytimes.com/2016/07/13/business/economy/antitrust-competition-inequality.html

[19] http://unctad.org/en/pages/PublicationWebflyer.aspx?publicationid=1852

[20] http://ohchr.org/EN/HRBodies/HRC/WGTransCorp/Session3/Pages/Session3.aspx

[21] See paragraph 35 of the report at:
http://ohchr.org/Documents/HRBodies/HRCouncil/WGTransCorp/Session3/DraftReportThirdSession.docx

[22] Pages 12 and 24 of the cited ITC paper.

[23] Page 14 of the cited ITC paper; see also page 46 of the cited UNCTAD report; see also paragraphs 42-43 and 48-52 of the cited February 2018 Secretariat Note.

[24] Page 19 of the cited ITC paper; see also pages 46 and 86 of the cited UNCTAD report; see also paragraphs 53-55 of the cited February 2018 Secretariat Note.

[25] Page 24 of the cited ITC paper.

[26] Paragraph 3.3 of "Statement by the African Group", WTO document JOB/GC/144, 20 October 2017.

digital industrial policies such as subsidies, R&D subsidies, development of, and access to, and ownership of technologies, economies of scale, government-sponsored infrastructure, tax benefits, etc.[27]

Proposals such as ensuring the free flow of data, no data localisation requirements, permanent moratorium on customs duties, non-disclosure of source code, barring forced technology transfer, etc. are not likely to be helpful for MSMEs in Africa[28] or elsewhere[29].

In fact, it has been said that[30]:

> … at present, the theme of MSMEs is mostly pushed by the major economic powers advocating new binding disciplines and increased market access. In particular, new WTO E-commerce disciplines are being pushed by the international business community (represented by the International Chamber of Commerce (ICC)/B20) as an MSME issue. However, this E-commerce MSME agenda is in fact the agenda of large corporations. The envisaged binding E-commerce rules would subject MSMEs in developing countries to competition with the digital giants even as these developing countries' MSMEs face very real digital and technological challenges and would need policy space to establish their own domestic and regional E-commerce platforms. If rules would in fact serve developing countries' MSMEs, these should be binding technology transfer arrangements to bridge the digital and technology divides, and binding financial assistance for infrastructure. However, these are not the type of rules being proposed.

As stated in paragraph 3 of the cited February 2018 Secretariat Note:

> In order to harness digitalization in support of trade, investments in information and communications technology (ICT) infrastructure should be complemented by an appropriate set of regulations and institutions, and support for skills development. Current gaps in terms of e-commerce readiness, between and within countries, imply that benefits from e-commerce are not equally distributed.

As stated in paragraph 26 of the cited February 2018 Secretariat Note:

> The use of digital platforms has economic, social and political impacts. Policymakers face challenges in relation to relevant policy areas, such as competition and consumer protection, data protection, taxation and labour relations. Some policies and regulations may need adaptation to the new digital context. Although it may appear that most of the activities involved in the platform-based economy are free from any regulation, as long as these are economic activities, there would appear to be no reason to separate them from other traditional economic activities that are subject to existing policies and regulations. Thus, they should be regulated in a manner consistent with a fair trading environment that is not biased towards or against any modality of trade and that provides equivalent protection to the rights of all parties involved – consumers, workers and taxpayers.

---

[27] Paragraph 3.4 of the cited Statement by the African Group.

[28] Paragraph 3.5 of the cited Statement by the African Group.

[29] Page 5 of South Center (2017) "Micros, Small, and Medium-Sized Enterprises (MMSEs)", Analytical Note SC/AN/TDP/2017/4, July 2017, available at: https://www.southcentre.int/wp-content/uploads/2017/08/AN_TDP_2017_4_Micro-Small-and-Medium-sized-Enterprises-MSMEs_EN.pdf

[30] Page 1 of the cited South Center Analytical Note.

Regarding taxation, as stated in paragraph 33 of the cited February 2018 Secretariat Note:

> Policymakers in developing and developed countries alike face the challenge of taxation in the digital economy. Reliance on digital platforms may weaken the international tax concept that allocates jurisdictional tax claims over profits of multinational companies based on physical presence. It raises issues such as enforcement, where to tax non-resident e-commerce businesses, how to assess intra-group transactions, how to classify digital goods, how to identify taxpayers, and where and how to collect consumption tax. Whereas concerns related to tax implications from e-commerce are likely to be more pronounced in countries where the uptake of e-commerce is high, finding ways to address related concerns are of relevance to all countries.

We address the questions of focus in the following sections:

2. How can developing countries foster local platforms for domestic and cross-border e-commerce?
3. How can developing countries foster local platforms for domestic and cross-border e-commerce?
4. What are the good practices that developed and developing countries, including the least developed countries, can learn from each other?

Before doing that, we note as a preliminary matter that, as my colleague Parminder Jeet Singh puts the matter[31]:

> A global digital order is gradually and steadily taking shape. Various social sectors are getting transformed by digital "platforms", like the information sector by Google, commerce by Amazon, and urban transportation by Uber. Companies that own these platforms are largely multinational, US based monopolies. They soak up free raw data from developing countries and convert it into "digital intelligence", which is employed in reorganisation and consequent domination of all sectors. Apart from becoming a sustained model of economic exploitation of developing countries, this new form of digital dependency also carries dire political, social and cultural consequences.
>
> Viewing the digital phenomenon through narrow frameworks of a promising industry and/or neutral tool for socioeconomic development, developing countries have ignored larger policy issues like internalising network effects of data and digital intelligence to support national industry, regulation of platforms, and ownership of publicly important digital data.

[31] Parminder Jeet Singh (2017) *Developing Countries in the Emerging Global Digital Order – A Critical Geopolitical Challenge to which the Global South Must Respond*, available at: http://itforchange.net/sites/default/files/Developing-Countries-in-the-Emerging-Global-Digital-Order.pdf

2. How can developing countries foster e-commerce?

The key elements of developmental aspects of e-commerce are well captured in an article on the development aspects of the Internet by Constance Bommelaer (ISOC) and Tereza Horesjova (DiploFoundation) [32]:

- **Expanding infrastructure**: Private sector needs to invest for the infrastructure to provide Internet access and to create and host services, leaving to governments to prioritize areas with high costs or low demand.
- **Fostering skills and entrepreneurship**: A skilled technical community is necessary to deploy and operate access and content infrastructure. It is also necessary to develop human capacity so that there are entrepreneurs, developers and others to create content and services and the innovative new business and delivery models built on them.
- **Developing a supportive governance system**: Good governance is needed to set the principles and rules of an enabling environment for a local Internet ecosystem, and specific policies to promote infrastructure investment and human capacity. Governments can also deploy their own content and services and encourage people to make the most of the Internet.

A key point made in that article – with which we agree – is that, while expanding infrastructure is a necessary step, it is not sufficient. Other steps need to be taken, in particular capacity building, making more local content available, but also maintaining trust, protecting data privacy, consumer protection, transparency, and the ability to communicate confidentially.[33] Local platforms should be fostered.[34]

Internet growth rates are slowing down[35]. While this is not necessarily an issue in parts of the world where most of the population is already connected, it is a serious issue for developing countries, where significant proportions of the population are not connected. Lack of trust may be a factor in discouraging access to the Internet. As the Internet Society puts the matter[36]:

> The slowdown in Internet growth rates, particularly in regions that were already falling behind the global average, lends urgency to the Internet Society's objective to connect the unconnected. There is evidence that existing users are increasingly concerned about privacy and security issues worldwide, and this may start to spill over to new users, who might become more reluctant to go online. If people trust the Internet, they are more likely to use it. Trust is at the heart of the Internet economy, and more and more at the heart of economic growth. This lends urgency to our objective to promote and restore trust in the Internet.

We discuss below the following issues, and provide specific recommendations regarding how to address them:

1. Cost of connectivity

---

[32] http://www.huffingtonpost.com/constance-bommelaer-de-leusse/internet-and-development-_1_b_12468308.html

[33] https://www.internetsociety.org/blog/asia-pacific-bureau/2016/10/cybersecurity-and-access-top-two-policy-concerns-asia-pacific

[34] Paragraphs 57-58 of the cited February 2018 Secretariat Note.

[35] See p. 33 of Internet Society (2016), Global Internet Report 2016, available at: https://www.internetsociety.org/globalinternetreport/2016/

[36] P. 34 of the cited ISOC Global Internet Report 2016

2. The economic and social value of data and its processing
3. Maintaining trust
4. Platform dominance
5. Job destruction and wealth concentration induced by e-commerce
6. Ethical issues of automation

2.1 Cost of connectivity

We cite from paragraph 41 of the Outcome document of the high-level meeting of the General Assembly on the overall review of the implementation of the outcomes of the World Summit on the Information Society, A/Res/70/125[37] (emphasis added):

> We reaffirm the commitment set out in the Geneva Declaration of Principles and the Tunis Commitment to the universality, indivisibility, interdependence and interrelation of all human rights and fundamental freedoms, including the right to development, as enshrined in the Vienna Declaration and Programme of Action of the World Conference on Human Rights.

It is not disputed that the ability to connect to the Internet is an important component of enabling the right to development. But, for development to take place, the cost of connecting must be affordable. Therefore, it is important to stress that reducing the cost of connectivity must be a priority: see paragraph 63 of the cited February 2018 Secretariat Report.

We refer in this respect to our submission[38] to an ITU open consultation and, for convenience, we reproduce here the relevant portions:

> 2.1 According to the 2015 report[39] of The Alliance for an Affordable Internet[40]:
>
> "Bold steps are needed to accelerate connectivity among women, the poor, and other marginalised populations. Overcoming the challenges to access posed by income and gender inequalities will require policies designed with these populations in mind. Market forces cannot connect everyone — free or subsidised public access in tandem with digital education will be critical to enabling connectivity for populations left behind." (Emphasis added)
>
> 2.2 Many steps, albeit not bold steps, are described in Supplement 2 of Recommendation ITU-T D.50[41]. A somewhat bolder step is proposed in Recommendation ITU-T D.156[42]. WTSA-12 Opinion 1[43] invites Member States "to take all measures necessary for the effective implementation of Recommendation ITU-T D.156."
>
> 2.3 In our view, the elements of an enabling environment to promote affordable Internet access include implementation of D.156 and of the measures described in Supplement 2 of D.50.

---

[37] http://workspace.unpan.org/sites/Internet/Documents/UNPAN96078.pdf

[38] http://www.itu.int/en/council/cwg-internet/Pages/display-feb2016.aspx?ListItemID=13

[39] http://a4ai.org/affordability-report/

[40] See the press release at http://1e8q3q16vyc81g8l3h3md6q5f5e.wpengine.netdna-cdn.com/wp-content/uploads/2016/02/2015-16AffordabilityReport_PressRelease.pdf

[41] https://www.itu.int/rec/T-REC-D.50/e

[42] https://www.itu.int/rec/T-REC-D.156/e

[43] http://www.itu.int/pub/T-RES-T.1000-2012

> 2.4 Functional separation is also an important element, see section 8 of our previous submission to this group, available at:
>
> http://www.itu.int/en/Lists/CWGContributionmar2014/Attachments/25//CWG-March.pdf
>
> 2.5 Furthermore, we are of the view that the fostering of competition is an important element of an enabling environment to promote and affordable Internet, and that visibility and transparency of prices, in particular wholesales prices promotes competition. We would thus support proposals, such as those made in the preparatory process of the 2012 World Conference on International Telecommunications (WCIT) to encourage greater transparency in the pricing of international Internet interconnections.

Subsequent to the cited ITU open consultation, two new relevant recommendations were approved, at the World Telecommunication Standardization Assembly: D.52, Establishing and connecting Regional IXPs to reduce costs of International internet connectivity; and D.53, International aspects of universal service. It is regrettable that some developed countries formally objected to the approval of those recommendations and took a reservation on those recommendations, see section 1.4 below. D.52 enunciates well known best practices and addresses international issues; D.53 enunciates several best practices and also addresses international issues. It must be stressed that all ITU-T Recommendations are voluntary, so, from the legal point of view, there is no need to express an explicit reservation: no state or private company is under any obligation to implement any ITU-T Recommendation.

2.2 The economic and social value of data and its processing

It is obvious that personal data has great value when it is collected on a mass scale and cross-referenced.[44] An excellent discussion of this topic, with numerous references, is give 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 .

As paragraph 31 of the cited February 2018 Secretariat Note[45] puts the matter:

> The digital economy relies increasingly on the generation, storage, processing and transfer of data, both within and across national boundaries. Access to data and data analysis are becoming strategically important for the competitiveness of companies. In relation to the use of digital

---

[44] See for example pp. vii and 2 of the GCIG report, available at: http://ourinternet.org/sites/default/files/inline-files/GCIG_Final%20Report%20-%20USB.pdf . 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

[45] http://unctad.org/meetings/en/SessionalDocuments/tdb_ede2d2_en.pdf

platforms, there are concerns about how data flows can be harnessed, while at the same time addressing concerns related to privacy and security.

Indeed, the monetization of personal data drives today's Internet services and the provision of so-called free services such as search engines.[46] These developments have significant implications, in particular for developing countries.[47] Users should have greater control over the ways in which their data are used.[48] In particular, they should be able to decide whether, and if so how, their personal data are used (or not used) to set the prices of goods offered online.[49] It should not be permissible (as it may be at present) for companies to collect data even before users consent to the collection by clicking on a button in a form[50]. The Internet Society recommends the following[51]: "All users should be able to control how their data is accessed, collected, used, shared and stored. They should also be able to move their data between services seamlessly."

As the Supreme Court of India put the matter in a recent judgment finding that privacy is a fundamental right: "To put it mildly, privacy concerns are seriously an issue in the age of information."[52] The ethical

---

[46] 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

[47] http://twn.my/title2/resurgence/2017/319-320/cover03.htm ; see also page 12 of UNCTAD's *Information Economy Report 2017: Digitalization, Trade and Development*, http://unctad.org/en/pages/PublicationWebflyer.aspx?publicationid=1872

[48] See for example pp. 42, 106 and 113 of GCIG. See also http://www.internetsociety.org/policybriefs/privacy ; and http://www.faz.net/aktuell/feuilleton/debatten/the-digital-debate/shoshana-zuboff-secrets-of-surveillance-capitalism-14103616.html ; and http://ec.europa.eu/commission/2014-2019/oettinger/announcements/speech-conference-building-european-data-economy_en and http://webfoundation.org/2017/03/web-turns-28-letter/ and https://ec.europa.eu/futurium/en/system/files/ged/ec_ngi_final_report_1.pdf and https://www.internetsociety.org/blog/public-policy/2017/03/my-data-your-business and https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2017/17-03-14_Opinion_Digital_Content_EN.pdf and http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+COMPARL+PE-592.279+01+DOC+PDF+V0//EN&language=EN and https://www.reuters.com/article/us-facebook-spain-fine/facebook-fined-1-2-million-euros-by-spanish-data-watchdog-idUSKCN1BM1OU and and https://www.economist.com/news/leaders/21735021-dominance-google-facebook-and-amazon-bad-consumers-and-competition-how-tame

[49] https://www.theguardian.com/technology/2017/jun/04/surge-pricing-comes-to-the-supermarket-dynamic-personal-data

[50] https://gizmodo.com/before-you-hit-submit-this-company-has-already-logge-1795906081?null

[51] Page 107 of the 2017 Global Internet Report: Paths to Our Digital Future, available at : https://future.internetsociety.org/wp-content/uploads/2017/09/2017-Internet-Society-Global-Internet-Report-Paths-to-Our-Digital-Future.pdf

[52] Paragraph 171 on p. 248. Why this is the case is explained in detail in paragraphs 170 ff. on pp. 246 ff. of the judgment. The full text of the extensively researched 547-page judgment is at: http://supremecourtofindia.nic.in/pdf/LU/ALL%20WP(C)%20No.494%20of%202012%20Right%20to%20Privacy.pdf ; see also the good discussion in paragraphs 21-35, 88-97, and 103-112 of the 19 October 2017 Report of the

issues of current and future processing of personal data are well explained in a report of the Ethical Advisory Group of the European Data Protection Supervisors.[53]

The following joke[54] well illustrates what is happening:

> CALLER: Is this Gordon's Pizza?
> GOOGLE: No sir, it's Google Pizza.
> CALLER: I must have dialed a wrong number. Sorry.
> GOOGLE: No sir, Google bought Gordon's Pizza last month.
> CALLER: OK. I would like to order a pizza.
> GOOGLE: Do you want your usual, sir?
> CALLER: My usual? You know me?
> GOOGLE: According to our caller ID data sheet, the last 12 times you called you ordered an extra-large pizza with three cheeses, sausage, pepperoni, mushrooms and meatballs on a thick crust.
> CALLER: OK! That's what I want …
> GOOGLE: May I suggest that this time you order a pizza with ricotta, arugula, sun-dried tomatoes and olives on a whole wheat gluten free thin crust?
> CALLER: What? I detest vegetables.
> GOOGLE: Your cholesterol is not good, sir.
> CALLER: How the hell do you know?
> GOOGLE: Well, we cross-referenced your home phone number with your medical records. We have the result of your blood tests for the last 7 years.
> CALLER: Okay, but I do not want your rotten vegetable pizza! I already take medication for my cholesterol.
> GOOGLE: Excuse me sir, but you have not taken your medication regularly.
> According to our database, you only purchased a box of 30 cholesterol tablets once, at Drug RX Network, 4 months ago.
> CALLER: I bought more from another drugstore.
> GOOGLE: That doesn't show on your credit card statement.
> CALLER: I paid in cash.
> GOOGLE: But you did not withdraw enough cash according to your bank statement.
> CALLER: I have other sources of cash.
> GOOGLE: That doesn't show on your last tax return unless you bought them using an undeclared income source, which is against the law.
> CALLER: WHAT THE HELL?
> GOOGLE: I'm sorry, sir, we use such information only with the sole intention of helping you.
> CALLER: Enough already! I'm sick to death of Google, Facebook, Twitter, WhatsApp and all the others. I'm going to an island without internet, cable TV, where there is no cell phone service and no one to watch me or spy on me
> GOOGLE: I understand sir, but you need to renew your passport first. It expired 6 weeks ago…

Special Rapporteur on Privacy, document A/72/43103, http://www.ohchr.org/Documents/Issues/Privacy/A-72-43103_EN.docx

[53] https://edps.europa.eu/sites/edp/files/publication/18-01-25_eag_report_en.pdf

[54] http://www.jokesoftheday.net/joke-Google-s-pizza/2017051897

Current trends regarding usage of personal data suggest that it "can be used to automatically and accurately predict a range of highly sensitive personal attributes including: sexual orientation, ethnicity, religious and political views, personality traits, intelligence, happiness, use of addictive substances, parental separation, age, and gender"[55] and that, on the basis of such data, people might be assigned a score that determines not just what advertisements they might see, but also whether they get a mortgage for their home[56]. In fact, big data is already being used in ways that could lead to social control, see:

https://www.wired.com/story/age-of-social-credit/

The European Parliament appears to be concerned about such issues, according to a draft report on the proposal for a regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications.[57]

The Indian government has published a White Paper which provides a comprehensive analysis of the issues and data protection legislation adopted in various jurisdictions, see: http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_171127_final_v2.pdf

All states should have comprehensive data protection legislation.[58] The European Commission advocates "the principle that high data protection standards are an essential component of the further development of a global information society capable of promoting innovation, growth and social prosperity".[59]

The development of so-called "smart cities" might result in further erosion of individual control of personal data. As one journalist puts the matter[60]: "A close reading [of internal documentation and marketing materials] leaves little room for doubt that vendors ... construct the resident of the smart city as someone without agency; merely a passive consumer of municipal services – at best, perhaps, a generator of data that can later be aggregated, mined for relevant inference, and acted upon." Related

[55] http://www.pnas.org/content/110/15/5802.full#aff-1

[56] https://www.theguardian.com/commentisfree/2017/jun/18/google-not-gchq--truly-chilling-spy-network and https://www.socialcooling.com/

[57] See document 2017/0003(COD) of 9 June 2017, available at: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-%2f%2fEP%2f%2fNONSGML%2bCOMPARL%2bPE-606.011%2b01%2bDOC%2bPDF%2bV0%2f%2fEN

[58] See for example p. 42 of GCIG;
and section 5 of http://www.itu.int/en/council/cwg-internet/Pages/display-feb2016.aspx?ListItemID=70 . A summary of adoption of data protection and data privacy laws by country can be found at: http://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Data-Protection-Laws.aspx

[59] Section 3.3.1 of "Exchanging and Protecting Personal Data in a Globalised World", Communication from the European Commission to the European Parliament and the Council, COM(2017) 7 of 10.1.2017, available at: https://ec.europa.eu/newsroom/document.cfm?doc_id=41157

[60] https://www.theguardian.com/cities/2014/dec/22/the-smartest-cities-rely-on-citizen-cunning-and-unglamorous-technology

issues arise regarding the use of employee data by platforms (such as Uber) that provide so-called "sharing economy" services[61].

The same issues arise regarding the replacement of cash payments by various forms of electronic payments. It is important to maintain "alternatives to the stifling hygiene of the digital panopticon being constructed to serve the needs of profit-maximising, cost-minimising, customer-monitoring, control-seeking, behavior-predicting commercial"[62] companies.

Further, mass-collected data (so-called "big data"[63]) are increasingly being used, via computer algorithms, to make decisions that affect people's lives, such as credit rating, availability of insurance, etc.[64] The algorithms used are usually not made public so people's lives are affected by computations made without their knowledge based on data that are often collected without their informed consent. An excellent analysis of the human rights dimensions of algorithms is found in Council of Europe document MSI-NET(2016)06[65], which makes a number of recommendations for government actions.

It is important to avoid that "big data", and the algorithmic treatment of personal data, do not result in increased inequality[66] and increased social injustice[67] which would threaten democracy.[68] A balanced discussion of the issues in the context of urban centers is given in a well-researched 2017 white paper by

---

[61] See "Stop rampant workplace surveillance" on p. 12 of:
http://library.fes.de/pdf-files/id-moe/12797-20160930.pdf

[62] http://thelongandshort.org/society/war-on-cash

[63] An excellent overview of the topic is provided in the May 2014 report commissioned by then-US President Obama, "Big Data: Seizing Opportunities, Preserving Values", available at:
https://bigdatawg.nist.gov/pdf/big_data_privacy_report_may_1_2014.pdf . An academic analysis of the social and public interest aspects of big data is given in Taylor, L., Floridi, L., van der Sloot, B. eds. (2017) *Group Privacy: new challenges of data technologies*. Dordrecht: Springer, available at:
https://www.stiftung-nv.de/sites/default/files/group-privacy-2017-authors-draft-manuscript.pdf ;
see also the analysis and recommendations at:
https://medium.com/@AINowInstitute/the-10-top-recommendations-for-the-ai-field-in-2017-b3253624a7

[64] http://time.com/4477557/big-data-biases/?xid=homepage ; an academic discussion is at:
http://www.tandfonline.com/doi/full/10.1080/1369118X.2016.1216147 and in the individual articles in:
Information, Communication & Society, Volume 20, Issue 1, January 2017,
http://www.tandfonline.com/toc/rics20/20/1

[65] https://rm.coe.int/16806a7ccc

[66] https://inequality.org/facts/income-inequality/ and
http://wir2018.wid.world/files/download/wir2018-summary-english.pdf . The fundamental reasons for rising inequality have been well explained by Piketty, Thomas (2014) *Capital in the Twenty-First Century*, Harvard University Press, see the review at:
http://www.boundary2.org/2014/10/capitals-offense-laws-entrenchment-of-inequality

[67] Even a well-known business publication has recognized that there is a need to address the issue of social equality, see:
http://www.economist.com/news/briefing/21721634-how-it-shaping-up-data-giving-rise-new-economy ;

see also pp. 13 and 57 of https://bigdatawg.nist.gov/pdf/big_data_privacy_report_may_1_2014.pdf

[68] See Cathy O'Neil, *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*, Crown Publishing, 2016; article at:
https://www.wired.com/2016/10/big-data-algorithms-manipulating-us/

CITRIS Connected Communities Initiative.[69] See also the discussion on pp. 75 ff. of the 2017 Internet Society Global Internet Report: Paths to Our Digital Future[70].

As learned scholars have put the matter[71]:

> Without people, there is no data. Without data, there is no artificial intelligence. It is a great stroke of luck that business has found a way to monetize a commodity that we all produce just by living our lives. Ensuring we get value from the commodity is not a case of throwing barriers in front of all manner of data processing. Instead, it should focus on aligning public and private interests around the public's data, ensuring that both sides benefit from any deal.
>
> …
>
> A way of conceptualizing our way out of a single provider solution by a powerful first-mover is to think about datasets as public resources, with attendant public ownership interests.

Another way of putting it is to note that the use of data is an extractive industry analogous to the mining and oil industries: "No reasonable person would let the mining industry unilaterally decide how to extract and refine a resource, or where to build its mines. Yet somehow we let the tech industry make all these decisions [regarding data] and more, with practically no public oversight. A company that yanks copper out of an earth that belongs to everyone should be governed in everyone's interest. So should a company that yanks data out of every crevice of our collective lives."[72]

Control of large amounts of data may lead to dominant positions that impeded competition[73]. But such large data sets are valuable only because they combine data from many individuals. Thus the value of the data is derived from the large number of people who contributed to the data. Consequently, "data is an essential, infrastructural good that should belong to all of us; it should not be claimed, owned, or managed by corporations."[74]

While some national legislators and/or courts have taken steps to strengthen citizens' rights to control the way their personal data are used[75], to consider product liability issues related to data[76], and to

---

[69] http://citris-uc.org/wp-content/uploads/2017/07/Inclusive-AI_CITRIS_2017.pdf

[70] https://future.internetsociety.org/wp-content/uploads/2017/09/2017-Internet-Society-Global-Internet-Report-Paths-to-Our-Digital-Future.pdf

[71] Powles, J. and Hodson, H., Google DeepMind and health care in an age of algorithms, *Health and Technology*, 2017, pp. 1-17, Health Technol. (2017) doi:10.1007/s12553-017-0179-1, available at: http://link.springer.com/article/10.1007%2Fs12553-017-0179-1

[72] https://www.theguardian.com/world/2017/aug/23/silicon-valley-big-data-extraction-amazon-whole-foods-facebook

[73] https://www.wired.com/story/ai-and-enormous-data-could-make-tech-giants-harder-to-topple/ ; https://www.wired.com/story/google-artificial-intelligence-monopoly/

[74] https://www.theguardian.com/commentisfree/2016/dec/04/data-populists-must-seize-information-for-benefit-of-all-evgeny-morozov

[75] A good academic overview of the issues is found at: http://www.ip-watch.org/2016/10/25/personality-property-data-protection-needs-competition-consumer-protection-law-conference-says/

consider the impact of big data with respect to prohibitions of discrimination in hiring[77], there does not appear to be adequate consideration of this issue at the international level.[78] Yet failure to address the issue at the international level can have negative consequences, including for trade. As UNCTAD puts the matter[79]:

> Insufficient protection can create negative market effects by reducing consumer confidence, and overly stringent protection can unduly restrict businesses, with adverse economic effects as a result. Ensuring that laws consider the global nature and scope of their application, and foster compatibility with other frameworks, is of utmost importance for global trade flows that increasingly rely on the Internet.
>
> …
>
> For those countries that still do not have relevant laws in place, governments should develop legislation that should cover data held by the government and the private sector and remove exemptions to achieve greater coverage. A core set of principles appears in the vast majority of national data protection laws and in global and regional initiatives. Adopting this core set of principles enhances international compatibility, while still allowing some flexibility in domestic implementation. Strong support exists for establishing a single central regulator when possible, with a combination of oversight and complaints management functions and powers. Moreover, the trend is towards broadening enforcement powers, as well as increasing the size and range of fines and sanctions in data protection.

Indeed, the International Conference of Data Protection and Privacy Commissioners has "appealed to the United Nations to prepare a legal binding instrument which clearly sets out in detail the rights to data protection and privacy as enforceable human rights" [80].

At its 34th session, 27 February-24 March 2017, the Human Rights Council adopted a new resolution on the Right to privacy in the digital age[81]. That resolution calls for data protection legislation, in particular to prevent the sale of personal data of personal data without the individual's free, explicit and informed consent.[82] We also note that the BRICS Leaders Xiamen Declaration[83] (4 September 2017) stated in its

---

[76] http://www.wablegal.com/european-commission-publishes-roadmap-future-proof-eu-product-liability-directive/

[77] https://www.eeoc.gov/eeoc/meetings/10-13-16/index.cfm

[78] Indeed, a group of scholars has called for the creation of a charter of digital rights, see: http://www.dw.com/en/controversial-eu-digital-rights-charter-is-food-for-thought/a-36798258
See also the UNCTAD study at: http://unctad.org/en/PublicationsLibrary/dtlstict2016d1_en.pdf ; and http://www.economist.com/news/leaders/21721656-data-economy-demands-new-approach-antitrust-rules-worlds-most-valuable-resource and the balanced discussion in pp. 93-95 of UNCTAD's *Information Economy Report 2017: Digitalization, Trade and Development*, http://unctad.org/en/pages/PublicationWebflyer.aspx?publicationid=1872

[79] *Data protection regulations and international data flows: Implications for trade and development*, pp. xi-xii, available at: http://unctad.org/en/PublicationsLibrary/dtlstict2016d1_en.pdf

[80] https://icdppc.org/wp-content/uploads/2015/02/Montreux-Declaration.pdf

[81] http://www.un.org/ga/search/view_doc.asp?symbol=A/HRC/34/L.7/Rev.1

[82] See 5(f) and 5(k) of the cited Resolution

paragraph 13 (emphasis added): "We will advocate the establishment of internationally applicable rules for security of ICT infrastructure, data protection and the Internet that can be widely accepted by all parties concerned, and jointly build a network that is safe and secure."

As paragraph 32 of the cited February 2018 Secretariat Note[84] puts the matter:

> The current system for data protection is fragmented, with varying global, regional and national regulatory approaches. In addition, many developing countries still lack legislation in this area altogether. Instead of pursuing multiple initiatives, it would be preferable for global and regional organizations to concentrate on one unifying initiative or a smaller number of initiatives that are internationally compatible.

Regarding algorithmic use of data, what a UK parliamentary committee[85] said at the national level can be also transposed to the international level:

> After decades of somewhat slow progress, a succession of advances have recently occurred across the fields of robotics and artificial intelligence (AI), fuelled by the rise in computer processing power, the profusion of data, and the development of techniques such a 'deep learning'. Though the capabilities of AI systems are currently narrow and specific, they are, nevertheless, starting to have transformational impacts on everyday life: from driverless cars and supercomputers that can assist doctors with medical diagnoses, to intelligent tutoring systems that can tailor lessons to meet a student's individual cognitive needs.
>
> Such breakthroughs raise a host of social, ethical and legal questions. Our inquiry has highlighted several that require serious, ongoing consideration. These include taking steps to minimise bias being accidentally built into AI systems; ensuring that the decisions they make are transparent; and instigating methods that can verify that AI technology is operating as intended and that unwanted, or unpredictable, behaviours are not produced.

A more detailed discussion is given in paragraphs 5-76 of the 19 October 2017 Report of the Special Rapporteur on Privacy.[86]

The recommendations of a national artificial intelligence research and development strategic plan[87] can be transposed at the international level:

> **Strategy 3**: Understand and address the ethical, legal, and societal implications of AI. We expect AI technologies to behave according to the formal and informal norms to which we hold our fellow humans. Research is needed to understand the ethical, legal, and social implications of AI, and to develop methods for designing AI systems that align with ethical, legal, and societal goals.

---

[83] Available at: http://www.mea.gov.in/Uploads/PublicationDocs/28912_XiamenDeclaratoin.pdf

[84] http://unctad.org/meetings/en/SessionalDocuments/tdb_ede2d2_en.pdf

[85] http://www.publications.parliament.uk/pa/cm201617/cmselect/cmsctech/145/14502.htm

[86] Document A/72/43103, http://www.ohchr.org/Documents/Issues/Privacy/A-72-43103_EN.docx

[87] https://www.nitrd.gov/news/national_ai_rd_strategic_plan.aspx

> **Strategy 4**: Ensure the safety and security of AI systems. Before AI systems are in widespread use, assurance is needed that the systems will operate safely and securely, in a controlled, well-defined, and well-understood manner. Further progress in research is needed to address this challenge of creating AI systems that are reliable, dependable, and trustworthy.

Indeed members of the European Parliament have called for European rules on robotics and artificial intelligence, in order to fully exploit their economic potential and to guarantee a standard level of safety and security.[88]

And experts speaking at a conference[89] on Artificial Intelligence hosted by the ITU raised many of the issues raised in this paper[90], as did experts at the AI Now public symposium, hosted by the White House and New York University's Information Law Institute, July 7th, 2016[91], as did a report by the UK Royal Society[92], as did the Internet Society in pages 31 ff. of its 2017 Global Internet Report: Paths to Our Digital Future[93]. An academic treatment of the issues is given in Wachter, S., Mittelstadt, B., and Floridi, L. (2017) "Transparent, explainable, and accountable AI for robotics", *Science Robotics,* 31 May 2017, Vol. 2, Issue 6, eaan6080, DOI: 10.1126/scirobotics.aan6080[94]. See also pages 4-5 of UNCTAD's *Information Economy Report 2017: Digitalization, Trade and Development*[95] and one expert's[96] predictions for 2018.

We recommend that UNCTAD[97] and UNCITRAL should study the issues related to the economic and social value or data, in particular "big data" and the increasing use of algorithms (including artificial intelligence[98]) to make decisions[99], which issues include economic and legal aspects. In particular,

---

[88] See http://www.europarl.europa.eu/news/en/press-room/20170210IPR61808/robots-and-artificial-intelligence-meps-call-for-eu-wide-liability-rules and https://ec.europa.eu/digital-single-market/en/blog/future-robotics-and-artificial-intelligence-europe

[89] http://www.itu.int/en/ITU-T/AI/Pages/201706-default.aspx . The report of the event is at: https://www.slideshare.net/ITU/ai-for-good-global-summit-2017-report

[90] See for example the summary at: https://www.ip-watch.org/2017/06/13/experts-think-ethical-legal-social-challenges-rise-robots/ and http://news.itu.int/enhancing-privacy-security-and-ethics-of-artificial-intelligence/

[91] https://artificialintelligencenow.com/media/documents/AINowSummaryReport_3_RpmwKHu.pdf

[92] https://royalsociety.org/topics-policy/projects/machine-learning/

[93] https://future.internetsociety.org/wp-content/uploads/2017/09/2017-Internet-Society-Global-Internet-Report-Paths-to-Our-Digital-Future.pdf

[94] http://robotics.sciencemag.org/content/2/6/eaan6080

[95] http://unctad.org/en/pages/PublicationWebflyer.aspx?publicationid=1872

[96] https://www.diplomacy.edu/blog/2018predictions#5

[97] For a description of UNCTAD's work addressing related issues, see: http://unctad14.org/EN/pages/NewsDetail.aspx?newsid=31 and in particular: http://unctad.org/en/PublicationsLibrary/dtlstict2016d1_en.pdf ; we also note the newly created Intergovernmental Group of Experts on E-Commerce, see: http://unctad.org/en/Pages/MeetingDetails.aspx?meetingid=1437

[98] For a discussion of some of the issues related to AI, see: https://www.wired.com/2017/02/ai-threat-isnt-skynet-end-middle-class/?mbid=nl_21017_p3&CNDID=42693809 and

UNCITRAL should be mandated to develop model laws, and possibly treaties, on personal data protection[100], algorithmic transparency and accountability[101], and artificial intelligence[102]; UNCTAD should be mandated to develop a study on the taxation of robots[103].

---

https://www.technologyreview.com/s/608248/biased-algorithms-are-everywhere-and-no-one-seems-to-care/ ; and https://www.technologyreview.com/s/607955/inspecting-algorithms-for-bias/ ; and https://blogs.microsoft.com/blog/2018/01/17/future-computed-artificial-intelligence-role-society/ ; a good discussion of the issues and some suggestions for how to address them is found at: https://www.internetsociety.org/doc/artificial-intelligence-and-machine-learning-policy-paper

[99] Specific recommendations regarding how to address the issues are found in Section 8, Conclusions and Recommendations, of the September 2016 Council of Europe document "Draft Report on the Human Rights Dimensions of Algorithms" (MSI-NET(2016)06) , available at: https://rm.coe.int/16806a7ccc

[100] Such a model law could flesh out the high-level data security and protection requirements enunciated in 8.7 of Recommendation ITU-T Y.3000, Big data – Cloud computing based requirements and capabilities, available at: https://www.itu.int/rec/T-REC-Y.3600-201511-I/en ; the privacy principles enunciated in 6 of Recommendation ITU-T X.1275, Guidelines on protection of personally identifiable information in the application of RFID technology, available at: https://www.itu.int/rec/T-REC-X.1275/en ; the core principles found in p. 56 and 65 ff. of the cited UNCTAD study at: http://unctad.org/en/PublicationsLibrary/dtlstict2016d1_en.pdf ; the core principles on page 95 of UNCTAD's *Information Economy Report 2017: Digitalization, Trade and Development*, http://unctad.org/en/pages/PublicationWebflyer.aspx?publicationid=1872 ;and the core principles enunciated by the Supreme Court of India in paragraph 184 on p. 257 of its recent judgment at: http://supremecourtofindia.nic.in/pdf/LU/ALL%20WP(C)%20No.494%20of%202012%20Right%20to%20Privacy.pdf ; and the key principles found in Section V of the Indian White Paper (p. 214 of the PDF file, p. 204 of the document) available at: http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_171127_final_v2.pdf ; it should also consider the "Guidelines for the Regulation of Computerized Personal Data Files" adopted by the UN General Assembly resolution 45/95 of 14 December 1990; the Guidelines are at: http://www.refworld.org/pdfid/3ddcafaac.pdf ; the Resolution is at: http://www.un.org/documents/ga/res/45/a45r095.htm . A treaty could be based on Council of Europe Convention no. 108: Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, available at: http://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680078b37 ; and it could also consider the provisions in Chapter II of the African Union Convention on Cyber Security and Personal Data Protection, available at: https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf ; and the "Top 10 Principles for Workers' Data Privacy and Protection" published by UNI Global Union, at: http://www.thefutureworldofwork.org/media/35421/uni_workers_data_protection.pdf . Guidelines/best practices could be based on sections 3-9 of the Council of Europe's T-PD consultative committee's January 2017 *Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data*, available at: https://rm.coe.int/16806ebe7a .

[101] Such a model law/treaty could be flesh out the Principles for Algorithmic Transparency and Accountability published by the Association for Computing Machinery (ACM), see: https://www.acm.org/binaries/content/assets/public-policy/2017_usacm_statement_algorithms.pdf

[102] Such a model law/treaty could flesh out the Asilomar AI Principles developed by a large number of experts, see: https://futureoflife.org/ai-principles/ . It should take into account the "Top 10 Principles for Ethical Artificial

Further, dominant search platforms may, inadvertently or deliberately, influence election results, which may pose an issue for democracy.[104]

We recommend to invite UN HCHR to study the potential effects of platform dominance on elections and democracy.

2.3 Maintaining trust

E-commerce cannot flourish without trust. Several issues must be addressed in order to maintain trust:

1. Externalities arising from lack of security
2. The Internet of Things (IoT)
3. Privacy, encryption and inappropriate mass surveillance

2.3.1 Externalities arising from lack of security and how to internalize such externalities

Security experts have long recognized that lack of ICT security creates a negative externality.[105] For example, if an electronic commerce service is hacked and credit card information is disclosed, the users of the service users will have to change their credit cards. This is a cost both for the user and for the credit card company. But that cost is not visible to the electronic commerce service. Consequently, the electronic commerce service does not have an incentive to invest in greater security measures.[106] Another, very concrete, example is provided by a software manufacturer's decision to stop correcting security problems in old versions of its software, with the consequence that a large number of computers were affected.[107] The cost of the attack was borne by the end-users, not by the software manufacturer.

Intelligence" published by UNI Global Union, at:
http://www.thefutureworldofwork.org/media/35420/uni_ethical_ai.pdf .

[103] http://www.bilan.ch/xavier-oberson/taxer-robots ; and
http://fortune.com/2017/02/18/bill-gates-robot-taxes-automation/ ; and
http://uk.businessinsider.com/bill-gates-robots-pay-taxes-2017-2

[104] https://newint.org/features/2016/07/01/can-search-engine-rankings-swing-elections/ and
https://www.theguardian.com/world/2016/oct/27/angela-merkel-internet-search-engines-are-distorting-our-perception and
http://singularityhub.com/2016/11/07/5-big-tech-trends-that-will-make-this-election-look-tame/ and
http://money.cnn.com/2016/11/09/technology/filter-bubbles-facebook-election and
http://www.pnas.org/content/112/33/E4512.full.pdf ; and
https://www.theguardian.com/technology/2016/dec/04/google-democracy-truth-internet-search-facebook and the comments starting at 13 minutes, 30 seconds, in the excellent talk at:
https://www.ted.com/talks/zeynep_tufekci_we_re_building_a_dystopia_just_to_make_people_click_on_ads/ ;
for a possible impact on free speech, see:
http://www.globalresearch.ca/google-corporate-press-launch-attack-on-alternative-media/5557677 .

[105] 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

[106] See also pp. vii and 66 of GCIG.

[107] https://en.wikipedia.org/wiki/WannaCry_cyber_attack

As the Global Internet Report 2016 of the Internet Society puts the matter[108]:

> There is a market failure that governs investment in cybersecurity. First, data breaches have externalities; costs that are not accounted for by organisations. Second, even where investments are made, as a result of asymmetric information, it is difficult for organizations to convey the resulting level of cybersecurity to the rest of the ecosystem. As a result, the incentive to invest in cybersecurity is limited; organisations do not bear all the cost of failing to invest, and cannot fully benefit from having invested.

There can be little doubt that many organizations are not taking sufficient measures to protect the security of their computer systems, see for example the May 2017 attack[109] that affected a large number of users and many hospitals.

As the European Union Agency for Network and Information Security (ENISA) puts the matter[110]: "Today we are seeing a **market failure for cybersecurity and privacy**: trusted solutions are more costly for suppliers and buyers are reluctant to pay a premium for security and privacy" (emphasis in original).

As explained below, the externalities arising from lack of security are exacerbated by the Internet of Things (IoT)[111]. As a well known security expert puts the matter[112]: "Security engineers are working on technologies that can mitigate much of this risk, but many solutions won't be deployed without government involvement. This is not something that the market can solve. ... the interests of the companies often don't match the interests of the people. ... Governments need to play a larger role: setting standards, policing compliance, and implementing solutions across companies and networks."

Recent research shows that a perceived lack of security is reducing consumer propensity to use the Internet for certain activities.[113]

---

[108] See p. 18 of the cited Global Internet Report 2016.

[109] https://en.wikipedia.org/wiki/WannaCry_cyber_attack

[110] Preamble of https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/infineon-nxp-st-enisa-position-on-cybersecurity

[111] See p. 107 of the cited Global Internet Report 2016.

[112] https://www.schneier.com/blog/archives/2016/07/real-world_secu.html

[113] https://www.cigionline.org/internet-survey ; and
pages 22 of UNCTAD's *Information Economy Report 2017: Digitalization, Trade and Development*, http://unctad.org/en/pages/PublicationWebflyer.aspx?publicationid=1872

Some national authorities are taking some measures.[114] In particular, the President of the USA issued an Executive Order[115] on 11 May 2017 that states:

> [certain high officials will lead] an open and transparent process to identify and promote action by appropriate stakeholders to improve the resilience of the internet [sic] and communications ecosystem and to encourage collaboration with the goal of dramatically reducing threats perpetrated by automated and distributed attacks (e.g., botnets).
>
> ...
>
> As a highly connected nation, the United States is especially dependent on a globally secure and resilient internet [sic] and must work with allies and other partners toward maintaining the policy set forth in this section.

ENISA is recommending[116] the development of "So called **baseline requirements** for IoT security and privacy that cover the essentials for trust, e.g. rules for authentication / authorization, should set **mandatory reference levels for trusted IoT solutions**." And it is recommending that the European Commission encourage "**the development of mandatory staged requirements for security and privacy in the IoT, including some minimal requirements.**" (Emphases in original)

Despite those national or regional initiatives, at present, there does not appear to be adequate consideration of these issues at either the national (in many countries) or international levels. In June 2016, German Chancellor Merkel called[117] for international regulations for digital markets, and in particular for international standards and rules for security; and one expert[118] predicts that the topic will get increasing attention in 2018. See also the statement by a major software company to the effect that "we must also ensure that there are robust, accountable, and transparent systems in place to ensure that governments are sharing information about vulnerabilities back out to affected companies."[119]

We recommend to invite IETF, ISOC, ITU, UNCITRAL, and UNCTAD to study the issue of externalities arising from lack of security, which has technical, economic, and legal aspects. In particular, UNCITRAL should be mandated to develop a model law on the matter.

---

[114] For example, for cybersecurity for motor vehicles, see: http://www.nhtsa.gov/About-NHTSA/Press-Releases/nhtsa_cybersecurity_best_practices_10242016 . For a general approach see Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC

[115] Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, available at: https://www.whitehouse.gov/the-press-office/2017/05/11/presidential-executive-order-strengthening-cybersecurity-federal

[116] 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

[117] http://www.rawstory.com/2017/06/germanys-merkel-says-digital-world-needs-global-rules/

[118] https://www.diplomacy.edu/blog/2018predictions#2

[119] https://blog.mozilla.org/netpolicy/2017/10/03/vulnerability-disclosure-should-be-in-new-eu-cybersecurity-strategy/

Further, as stated by the President of a leading software company (Microsoft)[120]:

> 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.
>
> In short, the time has come for governments to adopt a Digital Geneva Convention to protect civilians on the internet.
>
> …
>
> … governments around the world should pursue a broader multilateral agreement that affirms recent cybersecurity norms as global rules. Just as the world's governments came together in 1949 to adopt the Fourth Geneva Convention to protect civilians in times of war, we need a Digital Geneva Convention that will commit governments to implement the norms that have been developed to protect civilians on the internet in times of peace.
>
> Such a convention should commit governments to avoiding cyber-attacks 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.
>
> In addition, a Digital Geneva Convention needs to create an independent organization that spans the public and private sectors. Specifically, the world needs an independent organization that can investigate and share publicly the evidence that attributes nation-state attacks to specific countries.
>
> While there is no perfect analogy, the world needs an organization that can address cyber threats in a manner like the role played by the International Atomic Energy Agency in the field of nuclear non-proliferation. This organization should consist of technical experts from across governments, the private sector, academia and civil society with the capability to examine specific attacks and share the evidence showing that a given attack was by a specific nation-state. Only then will nation-states know that if they violate the rules, the world will learn about it.

In a press conference on 11 May 2017[121], the official presenting the cited US Executive Order[122] stated:

> ... I think the [security] trend is going in the wrong direction in cyberspace, and it's time to stop that trend ... . We've seen increasing attacks from allies, adversaries, primarily nation states but also non-nation state actors, and sitting by and doing nothing is no longer an option.

---

[120] https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/#sm.00017arazqit2faipqq2lyngzmxx4

[121] https://www.whitehouse.gov/the-press-office/2017/05/11/press-briefing-principal-deputy-press-secretary-sarah-sanders-and

[122] Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, available at: https://www.whitehouse.gov/the-press-office/2017/05/11/presidential-executive-order-strengthening-cybersecurity-federal

...

> ... [several] nation states are motivated to use cyber capacity and cyber tools to attack our people and our governments and their data. And that's something that we can no longer abide. We need to establish the rules of the road for proper behavior on the Internet, but we also then need to deter those who don't want to abide by those rules.

Following the WannaCrypt attack[123] in mid-May 2017, Microsoft reinforced its call for action, stating[124]:

> Finally, this attack provides yet another example of why the stockpiling of vulnerabilities by governments is such a problem. This is an emerging pattern in 2017. We have seen vulnerabilities stored by the CIA show up on WikiLeaks, and now this vulnerability stolen from the NSA has affected customers around the world. Repeatedly, exploits in the hands of governments have leaked into the public domain and caused widespread damage. An equivalent scenario with conventional weapons would be the U.S. military having some of its Tomahawk missiles stolen. And this most recent attack represents a completely unintended but disconcerting link between the two most serious forms of cybersecurity threats in the world today – nation-state action and organized criminal action.
>
> The governments of the world should treat this attack as a wake-up call. They need to take a different approach and adhere in cyberspace to the same rules applied to weapons in the physical world. We need governments to consider the damage to civilians that comes from hoarding these vulnerabilities and the use of these exploits. This is one reason we called in February for a new "Digital Geneva Convention" to govern these issues, including a new requirement for governments to report vulnerabilities to vendors, rather than stockpile, sell, or exploit them.

Civil society organizations have also called for treaty provisions to ensure that the Internet is used only for peaceful purposes.[125] A knowledgeable expert has explained the historical context for treaty-level provisions regarding cybersecurity.[126]

Indeed there is a long history of telecommunications (and by extension digital and cyber) security public international law since 1850, embodied in treaty instruments developed by the signatory nations of what is now known as the International Telecommunication Union (ITU), see:

http://www.emeraldinsight.com/doi/abs/10.1108/14636691111101856

We recommend to invite the UN General Assembly to consider the appropriate ways and means to convene a treaty-making conference to develop and adopt a binding treaty on norms to protect civilians against cyber-attacks, in times of peace, and to consider whether to develop a new treaty, or whether to

---

[123] https://en.wikipedia.org/wiki/WannaCry_cyber_attack

[124] https://blogs.microsoft.com/on-the-issues/2017/05/14/need-urgent-collective-action-keep-people-safe-online-lessons-last-weeks-cyberattack/#sm.00017arazqit2faipqq2lyngzmxx4 ; see also: https://www.wired.com/2017/05/microsoft-right-need-digital-geneva-convention/

[125] See point 5 of the Delhi Declaration, at https://justnetcoalition.org/delhi-declaration ; see also http://twn.my/title2/resurgence/2017/319-320/cover08.htm

[126] http://www.circleid.com/posts/20180108_china_pursuit_of_public_international_cybersecurity_law_leadership/

invite the ITU to integrate such norms into its own instruments, for example the International Telecommunication Regulations.

2.3.2 Internet of Things (IoT)

In the current environment, it can be expected that networked devices (the so-called Internet of Things – IoT)[127] will transmit data to manufacturers and service providers with little or no restrictions on the use of the data.[128] The recipients of the data could then correlate the data and resell it, as is currently the case for data collected by so-called free services such as search engines. Further, national surveillance programs could acquire such data and use it to construct profiles of individuals.

Such uses of data that are collected automatically for a specific purpose could have wide-reaching and unforeseen consequences.[129]

Further, interconnected devices may make decisions affecting daily life,[130] and this may call for the development of a regulatory framework to protect the interests of citizens. In particular, the issue of product liability may require changes to existing legal regimes.[131]

Increasingly, the safety of IoT devices will be affected by their security.[132] Thus, the security risks[133] posed by interconnected devices may require government actions.[134] For example, there may be a need

---

[127] A good overview of the technology, and the issues it raises, can be found at: http://www.internetsociety.org/doc/iot-overview ; a more detailed account is at: http://www.gao.gov/assets/690/684590.pdf

[128] See https://www.theguardian.com/technology/2015/jul/15/internet-of-things-mass-surveillance and the articles it references.

[129] See for example: http://www.itu.int/en/ITU-T/Workshops-and-Seminars/01072016/Documents/S1P3_Corinna_Schmitt_v3.pdf ; see also the "weaponization of everything", see p. 2 of GCIG.

[130] http://policyreview.info/articles/analysis/governance-things-challenge-regulation-law

[131] http://www.wablegal.com/european-commission-publishes-roadmap-future-proof-eu-product-liability-directive/

[132] https://www.iottechnews.com/news/2017/aug/04/why-iot-security-so-important-and-what-do-about-it/ ; and http://www.cl.cam.ac.uk/~rja14/Papers/weis2017.pdf and pages 5-6 of UNCTAD's *Information Economy Report 2017: Digitalization, Trade and Development*, http://unctad.org/en/pages/PublicationWebflyer.aspx?publicationid=1872 . A very good overview is given on p. 115 of ITU, Measuring the Information Society Report 2017, Vol. 1, at: https://www.itu.int/en/ITU-D/Statistics/Documents/publications/misr2017/MISR2017_Volume1.pdf and 2017 ENISA Baseline Security Recommendations for IoT at: https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot . For a comprehensive analysis, see the draft Report to the US President "Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats" at: https://www.ntia.doc.gov/files/ntia/publications/eo_13800_botnet_report_for_public_comment.pdf

[133] http://about.att.com/story/iot_cybersecurity_alliance.html ; see also http://www.businesswire.com/news/home/20170313005114/en/Tripwire-Study-96-Percent-Security-Professionals-Expect ; and pages 46 ff. and 73 of the Internet Society 2017 Global Internet Report: Paths to Our Digital Future, available at https://future.internetsociety.org/wp-content/uploads/2017/09/2017-Internet-Society-Global-Internet-Report-Paths-to-Our-Digital-Future.pdf

to provide incentives to those who make interconnected devices to make them secure: such incentives might be penalties for failure to build-in adequate security[135]. In this context, it is worth considering past experience with various devices, including electrical devices: they all have to conform to legal standards, all countries enforce compliance with such standards. It is not legitimate to claim that security and safety requirement stifle technological innovation. It must be recalled that the primary goal of private companies is to maximize profits. The purpose of regulation is to prevent profit-maximization from resulting in the production of dangerous products. As IBM Resilient Chief Technology Officer Bruce Schneier puts the matter[136], cybersecurity risks associated with the IoT require governmental intervention, as "the market is not going to fix this because neither the buyer nor the seller cares".

Since IoT products will be interconnected, at least to some degree, chaos can ensue if the products are not sufficiently secure[137] (e.g. all medical systems fail to work). Thus it is important to ensure that the products are sufficiently secure for mass deployment.

This is not a theoretical consideration. Insufficiently insecure IoT devices have already been used to perpetrate massive denial of service attacks, and such attacks could be used to bring down critical infrastructures.[138] As one security manager put the matter[139]: "In a relatively short time we've taken a system built to resist destruction by nuclear weapons and made it vulnerable to toasters." A thorough

---

[134] https://www.schneier.com/blog/archives/2016/07/real-world_secu.html and
https://www.scribd.com/document/328854049/DDoS-Letter-to-Chairman-Wheeler#download and
https://www.euractiv.com/section/innovation-industry/news/commission-plans-cybersecurity-rules-for-internet-connected-machines/ and
http://www.dailydot.com/layer8/bruce-schneier-internet-of-things/ and
https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/infineon-nxp-st-enisa-position-on-cybersecurity ;
https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/infineon-nxp-st-enisa-position-on-cybersecurity
and section section 6.2 of the 2017 ENISA Baseline Security Recommendations for IoT at:
https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot and the ISOC paper "IoT Security for Policymakers" (forthcoming).
For an academic discussion, see pp. 4 ff. of:
https://www.ntia.doc.gov/files/ntia/publications/k_farhat_ntia_iot.pdf

[135] http://www.wablegal.com/european-commission-publishes-roadmap-future-proof-eu-product-liability-directive/ . In the USA, the Federal Trade Commission (FTC) has invoked general consumer protection law to fine companies that do not have adequate online security, see *Wyndham vs. FTC*, at:
http://www2.ca3.uscourts.gov/opinarch/143514p.pdf

[136] https://digitalwatch.giplatform.org/updates/new-government-agencies-are-needed-deal-iot-security-regulations-says-ibm-resilient-cto and
http://searchsecurity.techtarget.com/news/450413107/Bruce-Schneier-Its-time-for-internet-of-things-regulation

[137] A particularly frightening scenario is presented at:
https://www.schneier.com/blog/archives/2016/11/self-propagatin.html

[138] See http://hothardware.com/news/latest-iot-ddos-attack-dwarfs-krebs-takedown-at-nearly-1-terabyte-per-second
http://hothardware.com/news/your-iot-device-could-be-part-of-a-ddos-botnet-how-to-shut-it-down
https://www.schneier.com/blog/archives/2016/09/someone_is_lear.html

[139] Jeff Jarmoc, head of security for global business service Salesforce, quoted in the excellent summary article at:
http://www.bbc.com/news/technology-37738823

study of the matter, which identifies gaps and contains recommendations for remedial actions, was published on 8 February 2017 by ENISA, see:

https://www.enisa.europa.eu/publications/m2m-communications-threat-landscape

In the US, a law[140] has been proposed to that would set minimum security standards for the government's purchase and use of a broad range IoT devices.[141] Related proposals are found in a draft report to the US President.[142]

But ICTs in general, and the Internet in particular, are global phenomena, so minimum security standards must also be global (or at least importing products that don't comply with internationally agreed standards should be prohibited), otherwise there will be a race to produce products in jurisdictions that don't have minimum security standards.

As a draft Report to the US President puts the matter[143]:

> Significant enhancements to the resilience of the ecosystem cannot be achieved through domestic action alone. The United States should lead engagement with international partners through regular bilateral and multilateral engagements on cybersecurity by leveraging expertise within the federal D/As. …
>
> …
>
> International standardization could be particularly beneficial. Widely applicable international standards for IoT security could expand the market for products that contribute to the resilience of the ecosystem while leveling the playing field for American businesses. As the NSTAC report recommended, industry and federal agencies that participate in standards development should coordinate on a strategy for engaging within appropriate industry-driven international standards bodies to ensure U.S. representation and leadership, and through that participation, champion a flexible and interoperable suite of international standards for IoT security.

At present, there does not appear to be adequate consideration of this issue at the international level.

We recommend to invite ITU, UNCITRAL and UNESCO to study issues related to IoT (including security of IoT devices, use of data from IoT devices, decisions made by IoT devices, etc.), which include technical, legal, and ethical aspects (for a partial list of such aspects, see Recommendation ITU-T Y.3001: Future networks: Objectives and design goals[144]). The studies should take into account Recommendation ITU-T

---

[140] https://www.scribd.com/document/355269230/Internet-of-Things-Cybersecurity-Improvement-Act-of-2017

[141] https://krebsonsecurity.com/2017/08/new-bill-seeks-basic-iot-security-standards/

[142] See Section III, Actions 1.2 and 1.4 at:
https://www.ntia.doc.gov/files/ntia/publications/eo_13800_botnet_report_for_public_comment.pdf

[143] Section III, Action 4.2 at:

https://www.ntia.doc.gov/files/ntia/publications/eo_13800_botnet_report_for_public_comment.pdf

[144] https://www.itu.int/rec/T-REC-Y.3001-201105-I

Y.3013: Socio-economic assessment of future networks by tussle analysis[145] as well as work in other bodes, in particular IEEE[146] and ENISA[147].

2.3.3 Privacy, encryption and prevention of inappropriate mass surveillance

Privacy is a fundamental right, and any violation of privacy must be limited to what is strictly necessary and proportionate in a democratic society.[148] Certain states practice mass surveillance that violates the right to privacy[149] (see for example A/HRC/31/64[150], A/71/373[151], A/HRC/34/60[152] and European Court of Justice judgment[153] ECLI:EU:C:2016:970 of 21 December 2016). As noted by the UN Human Rights Council Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, this can have negative effects on freedom of speech.[154]

The UN Human Rights Council Special Rapporteur on the right to privacy stated that he had "identified a serious obstacle to privacy in that there is a vacuum in international law in surveillance and privacy in cyberspace. ... It is not only the lack of substantive rules which are an obstacle to privacy promotion and protection, but also one of adequate mechanisms."[155] He also stated that the UN should discuss and adopt a new instrument to protect privacy rights.[156]

---

[145] http://www.itu.int/rec/T-REC-Y.3013-201408-I/en

[146] http://internetinitiative.ieee.org/images/files/resources/white_papers/internet_of_things_may_2017.pdf

[147] https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot

[148] See for example pp. vii, 32, 106 and 133 of GCIG; and 3(H) on p. 264 of the recent judgment of the Supreme Court of India, at
http://supremecourtofindia.nic.in/pdf/LU/ALL%20WP(C)%20No.494%20of%202012%20Right%20to%20Privacy.pdf

[149] For an academic discussion, see http://dx.doi.org/10.1080/23738871.2016.1228990 and
http://ijoc.org/index.php/ijoc/article/view/5521/1929 and the articles at
http://ijoc.org/index.php/ijoc/issue/view/13

[150] http://ohchr.org/Documents/Issues/Privacy/A-HRC-31-64.doc

[151] http://www.un.org/ga/search/view_doc.asp?symbol=A/71/373

[152] http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session34/Documents/A_HRC_34_60_EN.docx ; see in particular paragraphs 13-15, 18, 25 **and especially 42**.

[153] http://curia.europa.eu/juris/document/document.jsf?text=&docid=186492&doclang=EN ;
for a summary of the judgement, see:

http://www.commondreams.org/news/2016/12/21/eus-top-court-delivers-major-blow-mass-surveillance

[154] See paragraphs 17, 21, 22 and 78 of A/HRC/35/22 at
http://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/35/22

[155] Paragraph 4 of the 19 October 2017 Report of the Special Rapporteur on Privacy, document A/72/43103,
http://www.ohchr.org/Documents/Issues/Privacy/A-72-43103_EN.docx

[156] Paragraph 5 of the cited report.

As UNCTAD puts the matter[157]:

> countries need to implement measures that place appropriate limits and conditions on surveillance. Key measures that have emerged include:
>
> - providing a right to legal redress for citizens from any country whose data is transferred into the country (and subject to surveillance);
> - personal data collection during surveillance should be 'necessary and proportionate' to the purpose of the surveillance; and
> - surveillance activities should be subject to strong oversight and governance.

At its 34th session, 27 February-24 March 2017, the Human Rights Council (HRC) adopted a new resolution on the Right to privacy in the digital age[158]. That resolution recalls that States should ensure that any interference with the right to privacy is consistent with the principles of legality, necessity and proportionality.[159] Even a well-known business publication has recognized that privacy is a pressing issue[160]. And many of the issued mentioned in this contribution have been well presented in the 27 July 2017 Issue Paper "Online Privacy" of the Internet Society Asia-Pacific Bureau.[161]

The President of the United States has promulgated an Executive Order titled Enhancing Public Safety in the Interior of the United States. Its section 14 reads: "Privacy Act. Agencies shall, to the extent consistent with applicable law, ensure that their privacy policies exclude persons who are not United States citizens or lawful permanent residents from the protections of the Privacy Act regarding personally identifiable information."[162]

It appears to us that this decision and questions[163] related to its impact highlight the need to reach international agreement on the protection of personal data.

The same holds for a recent public admission that the agencies of at least one state monitor the communications of at least some accredited diplomats, even when the communications are with a private person ("... intelligence and law enforcement agencies ... routinely monitor the communications of [certain] diplomats" [164]). Surely there is a need to agree at the international level on an appropriate level of privacy protection for communications.

---

[157] *Data protection regulations and international data flows: Implications for trade and development*, p. 66, available at: http://unctad.org/en/PublicationsLibrary/dtlstict2016d1_en.pdf

[158] http://www.un.org/ga/search/view_doc.asp?symbol=A/HRC/34/L.7/Rev.1

[159] See 2 of the cited HRC Resolution

[160] http://www.economist.com/news/briefing/21721634-how-it-shaping-up-data-giving-rise-new-economy

[161] https://www.internetsociety.org/doc/issue-paper-asia-pacific-bureau-%E2%80%93-online-privacy

[162] https://www.whitehouse.gov/the-press-office/2017/01/25/presidential-executive-order-enhancing-public-safety-interior-united

[163] See for example: http://www.sophieintveld.eu/letter-to-eu-commission-what-impact-has-trump-decisions-on-privacy-shield-and-umbrella-agreement/

[164] https://www.washingtonpost.com/world/national-security/national-security-adviser-flynn-discussed-sanctions-with-russian-ambassador-despite-denials-officials-say/2017/02/09/f85b29d6-ee11-11e6-b4ff-ac2cf509efe5_story.html?utm_term=.63a87203f039

Encryption is a method that can be used by individuals to guarantee the secrecy of their communications. Some states have called for limitations on the use of encryption[165], or for the implementation of technical measures to weaken encryption. Many commentators have pointed out that any weakening of encryption can be exploited by criminals and will likely have undesirable side effects (see for example paragraphs 42 ff. of A/HRC/29/32[166]). Many commentators oppose state-attempts to compromise encryption.[167] The 2016 UNESCO Report "Human rights and encryption" also points out that attempts to limit the use of encryption, or to weaken encryption methods, may impinge on freedom of expression and the right to privacy.[168] The cited HRC resolution calls on states not to interfere with the use of encryption.[169] The Internet Society recommends the following[170]: "Encryption is and should remain an integral part of the design of Internet technologies, applications and services. It should not be seen as a threat to security. We must strengthen encryption, not weaken it." And this because "If governments persist in trying to prevent the use of encryption, they put at risk not only freedom of expression, privacy, and user trust, but the future Internet economy as well."[171]

At present, most users do not use encryption for their E-Mail communications, for various reasons, which may include lack of knowledge and/or the complexity of implementing encryption. There is a general need to increase awareness of ways and means for end-users to improve the security of the systems they use.[172]

Secrecy of telecommunications is guaranteed by article 37 of the ITU Constitution. However, this provision appears to be out of date and to require modernization[173]. In particular, restrictions must be placed on the collection and aggregation of meta-data.[174]

There does not appear to be adequate consideration of the issues outlined above at the international level.[175]

---

[165] See for example https://www.bloomberg.com/news/articles/2017-07-10/australia-s-turnbull-urges-internet-providers-to-block-extremism and https://www.diplomacy.edu/blog/2018predictions#9

[166] https://documents-dds-ny.un.org/doc/UNDOC/GEN/G15/095/85/PDF/G1509585.pdf?OpenElement

[167] See for example pp. vii, 106, and 113 of GCIG. See also http://science.sciencemag.org/content/352/6292/1398 ; http://www.internetsociety.org/policybriefs/encryption ; section 4 of http://www.itu.int/en/council/cwg-internet/Pages/display-feb2016.aspx?ListItemID=70 ; https://securetheinternet.org/ and http://dl.cryptoaustralia.org.au/Coalition+Letter+to+5eyes+Govs.pdf

[168] See in particular pp. 54 ff. The Report is at: http://unesdoc.unesco.org/images/0024/002465/246527e.pdf

[169] See 9 of the cited HRC Resolution

[170] Page 106 of the 2017 Global Internet Report: Paths to Our Digital Future, available at: https://future.internetsociety.org/wp-content/uploads/2017/09/2017-Internet-Society-Global-Internet-Report-Paths-to-Our-Digital-Future.pdf

[171] Page 39 of the cited ISOC report.

[172] See for example p. 66 of GCIG; and https://www.internetsociety.org/blog/2017/10/krack-reinforces-need-encryption-multiple-layers-stack/.

[173] For a specific proposal, see the last page of the proposals at: https://justnetcoalition.org/sites/default/files/HCHR_report_final.pdf

[174] See p. 31 of GCIG.

We recommend to invite IETF, ISOC, ITU, and OHCHR[176] to study the issues of privacy, encryption and prevention of inappropriate mass surveillance, which include technical, user education, and legal aspects.

2.4 How to deal with platform dominance

It is an observed fact that, for certain specific services (e.g. Internet searches, social networks, online book sales, online hotel reservations) one particular provider becomes dominant[177]. If a platform's dominance is due to a better service offer, then market forces are at work and there is no need for regulatory intervention. But, as paragraph 27 of the February 2018 Secretariat Note correctly states:

> Winner-takes-all dynamics are typical in platform-based economies, where network effects benefit first movers and standard setters. Whoever controls the platform also controls the distribution channel, and this can give the dominant platform (and data) owner considerable market power. Indeed, the world's top four companies by market capitalization are all leveraging digital platforms: Apple, Alphabet (Google), Microsoft and Amazon.com.

If the dominance is due to economies of scale and network effects[178], then a situation akin to a natural monopoly[179] might arise, there might be abuse of dominant market power[180], and regulatory

---

[175] See paragraph 46 of http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session34/Documents/A_HRC_34_60_EN.docx

[176] We note with gratitude that the Human Rights Council Special Rapporteur on Privacy has initiated work on a possible international legal instrument on surveillance, see: http://www.ohchr.org/Documents/Issues/Privacy/SurveillanceAndPrivacy.doc and http://www.ohchr.org/Documents/Issues/Privacy/DraftLegalInstrumentGovernmentLed.pdf

[177] 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/

[178] 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 . As paragraph 27 of the cited February 2018 Secretariat correctly puts the matter: "Winner-takes-all dynamics are typical in platform-based economies, where network effects benefit first movers and standard setters. Whoever controls the platform also controls the distribution channel, and this can give the dominant platform (and data) owner considerable market power. Indeed, the world's top four companies by market capitalization are all leveraging digital platforms: Apple, Alphabet (Google), Microsoft and Amazon.com." See http://unctad.org/meetings/en/SessionalDocuments/tdb_ede2d2_en.pdf

[179] https://en.wikipedia.org/wiki/Natural_monopoly

[180] 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/ and http://www.other-news.info/2018/02/amazon-doesnt-just-want-to-dominate-the-market-it-wants-to-become-the-market/ ; 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

intervention is required[181]. As paragraph 37 of the cited February 2018 Secretariat Note correctly states: "… there are concerns that the market power of certain platforms may lead to abuse of dominant positions, data protection and privacy issues, tax erosion and negative effects on jobs."

For example, platforms might abusively use personal data to set high prices for goods for certain customers, or a dominant national provider might impede the operation of an international competitor[182], or a dominant company may excessively influence governments[183], or a dominant search engine might provide search results that favor certain retail sites[184]. As the founders of Google put the matter back in 1998 (when they were graduate students): "we believe the issue of advertising causes enough mixed incentives that it is crucial to have a competitive search engine that is transparent and in the academic realm"[185].

---

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 .
Regarding the dangers of one company dominating artificial intelligence, see:
https://www.wired.com/story/google-artificial-intelligence-monopoly/ .

[181] A forceful and well-reasoned call for regulation has been given by *The Economist*, see:
http://www.economist.com/news/leaders/21721656-data-economy-demands-new-approach-antitrust-rules-worlds-most-valuable-resource and
https://www.economist.com/news/leaders/21735021-dominance-google-facebook-and-amazon-bad-consumers-and-competition-how-tame ; see also:
https://www.nytimes.com/2017/04/22/opinion/sunday/is-it-time-to-break-up-google.html ; and
https://www.ip-watch.org/2017/05/09/republica-2017-strategy-empire-revealed-patents/ and
pp. 52 ff. of http://www.autoritedelaconcurrence.fr/doc/reportcompetitionlawanddatafinal.pdf and
https://www.insidetechmedia.com/2017/11/07/the-bundeskartellamt-publishes-a-paper-on-big-data-and-competition/ .
For a high-level outline of the issues, see Recommendation ITU-T D.261, Principles for market definition and identification of operators with significant market power – SMP, at:
https://www.itu.int/rec/T-REC-D.261 .

[182] https://techcrunch.com/2016/11/28/ubers-china-app-is-now-separate-from-its-global-app-and-a-nightmare-for-foreigners/

[183] 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

[184] The European Commission found that Google had done this, see:
http://europa.eu/rapid/press-release_STATEMENT-17-1806_en.htm
http://europa.eu/rapid/press-release_MEMO-17-1785_en.htm ; as has the Competition Commission of India:
https://www.medianama.com/2018/02/223-google-fined-rs-136-crore-for-abusing-dominant-position-in-india/

[185] At the end of Appendix A of the paper by Brin and Page, "The Anatomy of a Large-Scale Hypertextual Web Search Engine" at http://infolab.stanford.edu/~backrub/google.html

Such corporate power can erode democracy, by in effect shifting power from the democratically elected representatives of the people to corporations, which not democratic entities. A scholarly article well documents the current trend towards shifting decision-making powers to private companies and concludes (the considerations below apply to many companies in addition to Amazon)[186]:

> Solutions to Amazon's power will, no doubt, be hard to advance as a political matter—consumers like 2-day deliveries. But understanding the bigger picture here is a first step. Political economy clarifies the stakes of Amazon's increasing power over commerce. We are not simply addressing dyadic transactions of individual consumers and merchants. Data access asymmetries will disadvantage each of them (and advantage Amazon as the middleman) for years to come. Nor can we consider that power imbalance in isolation from the way Amazon pits cities against one another. Mastery of political dynamics is just as important to the firm's success as any technical or business acumen. And only political organization can stop its functional sovereignties from further undermining the territorial governance at the heart of democracy.

As the Internet Society puts the matter on page 40 of its 2017 Global Internet Report: Paths to Our Future[187]: " … the scope of market change driven by dramatic advances in technology will inevitably force a fundamental rethink of existing approaches in competition law and traditional communications regulation. Data will increasingly be seen as an asset linked to competitive advantage, changing the nature of merger reviews, evaluations of dominance and, importantly, consumer protection."

Below are two quotes, one from the US, from WIRED, and another from an Asia tech market:

> Today's titans tower over their kingdoms, secure behind their walls of user data and benefiting from extreme network effects that make serious competition from startups nearly impossible. US antitrust laws, written in the industrial age, don't capture many of the new realities and potential dangers of these vast data empires. Maybe they should.[188]

> The era of startups in Southeast Asian ecommerce has seemingly ended. As Amazon and Alibaba pour their unlimited resources into the region, entrepreneurs starting their own marketplace today may be signing their bankruptcy filing.[189]

Further, as already noted, control of large amounts of data may lead to dominant positions that impeded competition[190]. As a learned commentator puts the matter[191]:

> Five American firms – China's Baidu being the only significant foreign contender – have already extracted, processed and digested much of the world's data. This has given them advanced AI

---

[186] https://lpeblog.org/2017/12/06/from-territorial-to-functional-sovereignty-the-case-of-amazon/

[187] https://future.internetsociety.org/wp-content/uploads/2017/09/2017-Internet-Society-Global-Internet-Report-Paths-to-Our-Digital-Future.pdf

[188] https://www.wired.com/story/what-microsofts-antitrust-case-teaches-us-about-silicon-valley/

[189] https://www.techinasia.com/southeast-asia-ecommerce-startups-giants

[190] https://www.wired.com/story/ai-and-enormous-data-could-make-tech-giants-harder-to-topple/

[191] https://www.theguardian.com/commentisfree/2016/dec/04/data-populists-must-seize-information-for-benefit-of-all-evgeny-morozov

capabilities, helping to secure control over a crucial part of the global digital infrastructure. Immense power has been shifted to just one sector of society as a result.

Appropriate regulatory intervention might be different from that arising under present competition or anti-trust policies.[192] As one commentator puts the matter[193] (his text starts with a citation):

> *"'I do not divide monopolies in private hands into good monopolies and bad monopolies. There is no good monopoly in private hands. There can be no good monopoly in private hands until the Almighty sends us angels to preside over the monopoly. There may be a despot who is better than another despot, but there is no good despotism'*
> William Jennings Bryan, speech, 1899, quoted in Hofstadter (2008)

> The digital world is currently out of joint. A small number of tech companies are very large, dominant and growing. They have not just commercial influence, but an impact on our privacy, our freedom of expression, our security, and – as this study has shown – on our civic society. Even if they mean to have a positive and constructive societal impact – as they make clear they do – they are too big and have too great an influence to escape the attention of governments, democratic and non-democratic. Governments have already responded, and more will."

As a scholar puts the matter[194]:

> … the current framework in antitrust—specifically its pegging competition to "consumer welfare," defined as short-term price effects—is unequipped to capture the architecture of market power in the modern economy. … Specifically, current doctrine underappreciates the risk of predatory pricing and how integration across distinct business lines may prove anticompetitive. These concerns are heightened in the context of online platforms for two reasons. First, the economics of platform markets create incentives for a company to pursue growth over profits, a strategy that investors have rewarded. Under these conditions, predatory pricing becomes highly rational—even as existing doctrine treats it as irrational and therefore implausible. Second, because online platforms serve as critical intermediaries, integrating across business lines positions these platforms to control the essential infrastructure on which their rivals depend. This dual role also enables a platform to exploit information collected on companies using its services to undermine them as competitors.

---

[192] https://www.competitionpolicyinternational.com/let-the-right-one-win-policy-lessons-from-the-new-economics-of-platforms/
https://www.washingtonpost.com/business/is-amazon-getting-too-big/2017/07/28/ff38b9ca-722e-11e7-9eac-d56bd5568db8_story.html .
An academic treatment of the topic is Khan, L. M. (2017) "Amazon's Antitrust Paradox", *The Yale Law Journal*, vol. 126, no. 3, pp. 564-907, available at: http://www.yalelawjournal.org/note/amazons-antitrust-paradox

[193] Martin Moore. *Tech Giants and Civic Power*. Centre for the Study of Media, Communication, and Power, King's College. April 2016. Available at:
http://www.kcl.ac.uk/sspp/policy-institute/CMCP/Tech-Giants-and-Civic-Power.pdf

[194] Khan, L. M. (2017) "Amazon's Antitrust Paradox", *The Yale Law Journal*, vol. 126, no. 3, pp. 564-907, available at:
http://www.yalelawjournal.org/note/amazons-antitrust-paradox

> … [This paper] closes by considering two potential regimes for addressing [a dominant player's] power: restoring traditional antitrust and competition policy principles or applying common carrier obligations and duties.

As a well-researched report put the matter: "[Company X's] increasing dominance comes with high costs. It's eroding opportunity and fueling inequality, and it's concentrating power in ways that endanger competition, community life, and democracy. And yet these consequences have gone largely unnoticed thanks to [Company X's] remarkable invisibility and the way its tentacles have quietly extended their reach."[195]

As noted above, the dominance of certain platforms[196] raises issues related to freedom of speech, because some platforms apply strict rules of their own to censor certain types of content[197], and, for many users, there are no real alternatives to dominant platforms[198]; and some workers might also face limited choices due to dominant platforms[199].

As *The Economist* puts the matter[200]:

> Prudent policymakers must reinvent antitrust for the digital age. That means being more alert to the long-term consequences of large firms acquiring promising startups. It means making it easier for consumers to move their data from one company to another, and preventing tech firms from unfairly privileging their own services on platforms they control (an area where the commission, in its pursuit of Google, deserves credit). And it means making sure that people have a choice of ways of authenticating their identity online.
>
> …
>
> … The world needs a healthy dose of competition to keep today's giants on their toes and to give those in their shadow a chance to grow."

As a well-known technologist reportedly stated in March 2017, the telecoms industry has evolved from a public peer-to-peer service – where people had the right to access telecommunications – to a pack of

---

[195] https://ilsr.org/amazon-stranglehold/

[196] For data regarding such dominance, see for example:
http://www.eecs.umich.edu/eecs/about/articles/2009/Observatory_Report.html
http://www.networkworld.com/article/2251851/lan-wan/the-internet-has-shifted-under-our-feet.html
http://www.xconomy.com/boston/2009/10/20/arbor-networks-reports-on-the-rise-of-the-internet-hyper-giants/
https://www.arbornetworks.com/blog/asert/the-battle-of-the-hyper-giants-part-i-2/

[197] See for example https://www.theguardian.com/technology/2016/sep/09/facebook-deletes-norway-pms-post-napalm-girl-post-row

[198] https://www.theguardian.com/technology/2016/nov/17/google-suspends-customer-accounts-for-reselling-pixel-phones

[199] https://www.nytimes.com/2017/03/21/magazine/platform-companies-are-becoming-more-powerful-but-what-exactly-do-they-want.html?_r=2

[200] http://www.economist.com/news/leaders/21707210-rise-corporate-colossus-threatens-both-competition-and-legitimacy-business

content delivery networks where the rules are written by a handful of content owners, ignoring any concept of national sovereignty.[201]

And, citing *The Economist* again[202]:

> The dearth of data markets will also make it more difficult to solve knotty policy problems. Three stand out: antitrust, privacy and social equality. The most pressing one, arguably, is antitrust …

As learned scholars have put the matter[203]:

> The question of how to make technology giants such as Google more publicly accountable is one of the most pressing political challenges we face today. The rapid diversification of these businesses from web-based services into all sorts of aspects of everyday life—energy, transport, healthcare—has found us unprepared. But it only emphasizes the need to act decisively.

An excellent overview of various methods that can be used to increase competition is provided in Wu, Tim, Antitrust Via Rulemaking: Competition Catalysts (October 24, 2017), *Colorado Technology Law Journal*.[204] Wu refers to actual examples (including in telecommunications) to show how regulations can be used to increase (or inadvertently fail to increase) completion. That is, regulatory intervention is means to be considered in parallel to, or instead of, judicial enforcement of antitrust/competition law.

Measures to ensure accountability may be needed with respect to labor-relation issues, and not only with respect to users and consumers.[205]

Large data sets are valuable only because they combine data from many individuals. Thus the value of the data is derived from the large number of people who contributed to the data. Consequently, "data is an essential, infrastructural good that should belong to all of us; it should not be claimed, owned, or managed by corporations."[206]

National authorities in a number of countries have undertaken investigations,[207] and even imposed measures,[208] in specific cases. And at least one influential member of a national parliament has

---

[201] https://disruptive.asia/transit-dead-content-literally-rules/

[202] http://www.economist.com/news/briefing/21721634-how-it-shaping-up-data-giving-rise-new-economy

[203] In section 4.5 of Powles, J. and Hodson, H., Google DeepMind and health care in an age of algorithms, *Health and Technology*, 2017, pp. 1-17, Health Technol. (2017) doi:10.1007/s12553-017-0179-1, available at: http://link.springer.com/article/10.1007%2Fs12553-017-0179-1

[204] https://ssrn.com/abstract=3058114

[205] https://www.nytimes.com/interactive/2017/04/02/technology/uber-drivers-psychological-tricks.html?_r=2

[206] https://www.theguardian.com/commentisfree/2016/dec/04/data-populists-must-seize-information-for-benefit-of-all-evgeny-morozov

[207] See for example http://europa.eu/rapid/press-release_IP-16-1492_en.htm ; http://europa.eu/rapid/press-release_IP-16-2532_en.htm and http://europa.eu/rapid/press-release_IP-15-5166_en.htm ;
a more general approach is described at:
http://www.accc.gov.au/media-release/accc-to-undertake-market-study-of-the-communications-sector

expressed concern about some major Internet companies "because they control essential tech platforms that other, smaller companies depend upon for survival."[209] The Legal Affairs Committee of the European Parliament adopted an Opinion in May 2017 that, among other provisions[210]:

> Calls for an appropriate and proportionate regulatory framework that would guarantee responsibility, fairness, trust and transparency in platforms' processes in order to avoid discrimination and arbitrariness towards business partners, consumers, users and workers in relation to, inter alia, access to the service, appropriate and fair referencing, search results, or the functioning of relevant application programming interfaces, on the basis of interoperability and compliance principles applicable to platforms;

The topic is covered to some extent in paragraphs 24 ff. of a European Parliament Committee Report on online platforms and the digital single market, (2016/2276(INI).[211] And by some provisions in the national laws of at least one country.[212] Many of the issues relating to platforms and human rights have been well documented by the IGF Dynamic Coalition on Platform Responsibility.[213]

However, it does not appear that there is an adequate platform for exchanging national experiences regarding such matters.[214]

Further, dominant platforms (in particular those providing so-called "sharing economy" services) may raise issues regarding worker protection, and some jurisdictions have taken steps to address such issues.[215]

We recommend to invite UNCTAD to study the economic and market issues related to platform dominance[216], and to facilitate the exchange of information on national and regional experiences, and

---

[208] See for example http://www.autoritedelaconcurrence.fr/user/standard.php?id_rub=606&id_article=2534 and, in the case of Google: http://europa.eu/rapid/press-release_IP-17-1784_en.htm

[209] http://www.cnet.com/news/senator-warren-says-apple-google-and-amazon-have-too-much-power/

[210] http://www.europarl.europa.eu/sides/getDoc.do?type=COMPARL&reference=PE-601.100&format=PDF&language=EN&secondRef=02

[211] http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+COMPARL+PE-599.814+01+DOC+PDF+V0//EN&language=EN

[212] See section 3.2 of the following commentary on the French Digital Republic Law:
https://www.lw.com/thoughtLeadership/French-digital-republic-law-english
see also the decrees issued in October 2017:
http://proxy-pubminefi.diffusion.finances.gouv.fr/pub/document/18/22764.pdf

[213] http://bibliotecadigital.fgv.br/dspace/handle/10438/19402

[214] Except for certain specific issues relating to Over the Top (OTT) services and telecommunications operators which are discussed in ITU. A good summary of those specific issues is found in the section on OTT services of:
http://www.itu.int/md/T13-WTSA.16-INF-0009/en

[215] See for example pp. 12 and 13 of http://library.fes.de/pdf-files/id-moe/12797-20160930.pdf and https://www.theguardian.com/technology/2016/oct/28/uber-uk-tribunal-self-employed-status and https://curia.europa.eu/jcms/upload/docs/application/pdf/2017-05/cp170050en.pdf .
A more general discussion of various issues arising out of platform dominance is at:
http://www.alainet.org/en/articulo/181307

that the ILO be mandated to study the worker protection issues related to platform dominance and the so-called "sharing economy".

2.5 How to deal with induced job destruction and wealth concentration

Scholars have documented the reduction in employment that has already been caused by automation[217]. It is likely that this trend will be reinforced in the future.[218] Even if new jobs are created as old jobs are eliminated, the qualifications for the new jobs are not the same as the qualifications for the old jobs.[219] And artificial intelligence can even result in the elimination of high-skilled jobs[220], including creation of software[221]. These developments, including the so-called sharing economy, pose

---

[216] We note in this context the existence in UNCTAD of the Intergovernmental Group of Experts on Competition Law and Policy, see:
http://unctad.org/en/Pages/DITC/CompetitionLaw/Intergovernmental-Group-of-Experts-on-Competition-Law-and-Policy.aspx
and the United Nations Set of Rules and Principles on Competition (TD/RBP/CONF/10/Rev.2), published in 2000 and available at:
http://unctad.org/en/docs/tdrbpconf10r2.en.pdf

[217] Paradoxically, automation has not increased productivity as much as would have been expected, and consequently it has resulted in stagnation of wages for most people and increasing income inequality, see: https://www.technologyreview.com/s/608095/it-pays-to-be-smart/ . For a good discussion of the large impact that digitalization will eventually have on manufacturing, see:
http://www.delivered.dhl.com/en/articles/2018/01/the-seismic-potential-of-digitalized-manufacturing.html

[218] http://robertmcchesney.org/2016/03/01/people-get-ready-the-fight-against-a-jobless-economy-and-a-citizenless-democracy/ and
http://www.newsclick.in/international/review-schiller-dan-2014-digital-depression-information-technology-and-economic-crisis and p. 88 of GCIG and
http://library.fes.de/pdf-files/wiso/12864.pdf and http://library.fes.de/pdf-files/wiso/12866.pdf and
http://unctad.org/en/PublicationsLibrary/presspb2016d6_en.pdf and
https://www.technologyreview.com/s/602869/manufacturing-jobs-arent-coming-back/ and
http://www.other-news.info/2017/03/the-robots-are-coming-your-jobs-are-at-risk/ and
https://www.nytimes.com/2017/03/28/upshot/evidence-that-robots-are-winning-the-race-for-american-jobs.html?_r=0 and
https://blogs.microsoft.com/blog/2018/01/17/future-computed-artificial-intelligence-role-society/ and
https://hackernoon.com/artificial-intelligence-3c6d80072416 .
While not necessarily related to ICTs, it is worrisome that the economic situation of least developed countries is deteriorating, see: http://unctad.org/en/PublicationsLibrary/ldc2016_en.pdf

[219] See for example p. viii of GCIG; see also http://www.economist.com/news/leaders/21701119-what-history-tells-us-about-future-artificial-intelligenceand-how-society-should ; and
https://www.technologyreview.com/s/601682/dear-silicon-valley-forget-flying-cars-give-us-economic-growth/ ;
https://www.technologyreview.com/s/602489/learning-to-prosper-in-a-factory-town/ : and
http://www.other-news.info/2017/01/poor-darwin-robots-not-nature-now-make-the-selection/ and
http://www.pwc.co.uk/services/economics-policy/insights/uk-economic-outlook.html and
http://www.pwc.co.uk/economic-services/YWI/pwc-young-workers-index-2017-v2.pdf and
http://www.worldbank.org/en/publication/wdr2016

[220] https://www.technologyreview.com/s/603431/as-goldman-embraces-automation-even-the-masters-of-the-universe-are-threatened/

[221] https://www.technologyreview.com/s/603381/ai-software-learns-to-make-ai-software/

policy and regulatory challenges[222], in particular for developing countries[223]. As the Internet Society puts the matter on page 35 of its 2017 Global Internet Report: Paths to Our Digital Future[224]: "The benefits of AI may also be unevenly distributed: for economies that rely on low-skilled labour, automation could challenge their competitive advantage in the global labour market and exacerbate local unemployment challenges, impacting economic development." See also the discussion on page 66 ff. of the cited report.

As paragraph 35 of the cited February 2018 Secretariat Note[225] puts the matter:

> … the fragmentation of the production process and a large oversupply of jobseekers on such [digital] platforms may weaken their bargaining power and thus accentuate tendencies towards a race to the bottom in terms of compensation and other working conditions. It is important that policies and regulations enable this expanding segment of the economy to provide quality and decent jobs.

Further, it has been observed that income inequality[226] is increasing in most countries, due at least in part to the deployment of ICTs[227]. More broadly, it is important to consider the development of ICTs in general, and the Internet in particular, from the point of view of social justice[228]. Indeed, it has been

---

[222] See for example p. 89 of GCIG. And the recent call for doing more to help globalization's losers by Mario Draghi, the president if the European Central Bank, Donald Tusk, the president of the European Council, and Christine Lagarde, the head of the International Monetary Fund, reported in the Financial Times: https://www.ft.com/content/ab3e3b3e-79a9-11e6-97ae-647294649b28 ; see also http://twn.my/title2/resurgence/2017/319-320/cover04.htm http://twn.my/title2/resurgence/2017/319-320/cover05.htm http://twn.my/title2/resurgence/2017/319-320/cover06.htm and Recommendation 2 of: https://artificialintelligencenow.com/media/documents/AINowSummaryReport_3_RpmwKHu.pdf and pp. 50-51 of UNCTAD's *Information Economy Report 2017: Digitalization, Trade and Development*, http://unctad.org/en/pages/PublicationWebflyer.aspx?publicationid=1872 .
The legal issues are well summarized in the 4 April 2017 report of the International Bar Association "Artificial Intelligence and Robotics and Their Impact on the Workplace", available at: https://www.ibanet.org/Article/NewDetail.aspx?ArticleUid=012a3473-007f-4519-827c-7da56d7e3509

[223] See for example http://twn.my/title2/resurgence/2017/319-320/cover01.htm and the UNCTAD Policy Brief No. 50 of October 2016 at http://unctad.org/en/PublicationsLibrary/presspb2016d6_en.pdf

[224] https://future.internetsociety.org/wp-content/uploads/2017/09/2017-Internet-Society-Global-Internet-Report-Paths-to-Our-Digital-Future.pdf

[225] http://unctad.org/meetings/en/SessionalDocuments/tdb_ede2d2_en.pdf

[226] See for example https://www.oxfam.org/en/research/working-few ; https://www.oxfam.org/en/research/economy-99 https://inequality.org/facts/income-inequality/. As the OECD put the matter in February 2018: "Income inequality in OECD countries is at its highest level for the past half century. … In emerging economies … the benefits of growth have not been evenly distributed and high levels of income inequality have risen further.", see: http://www.oecd.org/social/inequality.htm , accessed on 16 February 2018.

[227] See for example pp. 14, 20-21, and 118 ff. 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

[228] By "social justice" we mean the fair and just relation between the individual and society. This is measured by the explicit and tacit terms for the distribution of wealth, opportunities for personal activity and social privileges.

posited that the small number of individuals who control the wealth generated by dominant platforms (see below) may be using that wealth to further particular economic and political goals, and that such goals may erode social justice.[229] Further, the algorithms that are increasingly used to automate decisions such as granting home loans may perpetuate or even increase inequality and social injustice.[230]

At present, there does not appear to be adequate consideration of these issues at the international level, even if ILO[231] has recently started to address some of the issues.

We recommend to invite ILO and UNCTAD to study the issues of induced job destruction, wealth concentration, and the impact of algorithms on social justice and that UNCTAD compile and coordinate the studies made by other agencies such as OECD, World Bank, IMF.

2.6 Ethical issues of automation

More and more aspects of daily life are controlled by automated devices, and in the near future automated devices will provide many services that are today provided manually, such as transportation. Automated devices will have to make choices and decisions.[232] It is important to ensure that the choices and decisions comply with our ethical values. In this context, it is worrisome that some modern AI algorithms cannot be understood, to the point where it might be impossible to find out why an automated car malfunctioned[233].

According to one analysis, the new European Union Data Protection Regulation "will restrict automated individual decision-making (that is, algorithms that make decisions based on user-level predictors) which 'significantly affect' users. The law will also create a 'right to explanation,' whereby a user can ask for an explanation of an algorithmic decision that was made about them." [234] See also the discussion of algorithmic data processing and artificial intelligence presented above.

See https://en.wikipedia.org/wiki/Social_justice ;
a thorough discussion of the issues (impact on jobs, impact on income inequality, etc.), with many references, is found at: http://www.truth-out.org/news/item/40495-the-robot-economy-ready-or-not-here-it-comes .

[229] http://www.commondreams.org/news/2016/01/20/just-who-exactly-benefits-most-global-giving-billionaires-bill-gates and
http://www.thedailybeast.com/articles/2016/08/11/today-s-tech-oligarchs-are-worse-than-the-robber-barons.html .
A cogent analysis, which points out that the redistribution issues are global and not merely national (because nations that are advanced in terms of automation and artificial intelligence will reap the greatest economic benefits) is given at:
https://www.nytimes.com/2017/06/24/opinion/sunday/artificial-intelligence-economic-inequality.html

[230] https://www.fordfoundation.org/ideas/equals-change-blog/posts/weapons-of-math-destruction-data-scientist-cathy-o-neil-on-how-unfair-algorithms-perpetuate-inequality/

[231] http://www.other-news.info/2017/04/humanity-and-social-justice-a-must-for-the-future-of-work-ryder/ and
http://ilo.org/global/topics/future-of-work/WCMS_569528/lang--en/index.htm

[232] http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML%2BCOMPARL%2BPE-582.443%2B01%2BDOC%2BPDF%2BV0//EN

[233] https://www.technologyreview.com/s/604087/the-dark-secret-at-the-heart-of-ai/

[234] http://arxiv.org/abs/1606.08813

At present, some actions have been proposed at the national level[235], but there does not appear to be adequate consideration of these issues at the international level.

We recommend to invite UNESCO and UNICTRAL to study the ethical issues of networked automation, which include ethical and legal aspects.[236] As a starting point, the study should consider the IEEE Global Initiative for Ethical Considerations in Artificial Intelligence and Autonomous Systems. *Ethically Aligned Design: A Vision For Prioritizing Wellbeing With Artificial Intelligence And Autonomous Systems*, Version 1. IEEE, 2016[237]; and the recommendations of the AI Now 2017 Report[238].

3. Fostering local platforms

Economic issues other than the cost of connectivity are important. As noted in paragraphs 1.12 and 1.13 of our submission[239] to the cited ITU open consultation, the current dysfunctional intellectual property regime results in excessively high costs for hardware and software. Various reports[240] have recently highlighted that point in the context of human rights and development. As recent study put the matter[241]:

> … recent developments in copyright law attest to the need to rethink copyright in order to adapt its rules to its original dual character: as a right to secure and organize cultural participation and access to creative works on the one side, and as a guarantee for the creator to participate fairly in the fruit of the commercial exploitation of his or her works on the other. In these respects, it is proposed that copyright is to be (re)conceived as a right to access rather than a right to forbid, thereby emphasising the inclusive rather than the exclusive nature of copyright protection.

Use of open source software can help to ameliorate this situation. In that light, it is disappointing to note that many developed countries objected to the adoption of a resolution at the ITU World

---

[235] 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

[236] A commission of the European Parliament "Strongly encourages international cooperation in setting regulatory standards under the auspices of the United Nations" with respect to these issues, see 33 of the draft report cited in the previous footnote. See also:
http://www.thedrive.com/tech/11241/audi-ceo-calls-for-discussion-of-self-driving-car-ethics-at-united-nations-summit and
https://www.ip-watch.org/2017/06/13/experts-think-ethical-legal-social-challenges-rise-robots/ and
http://news.itu.int/enhancing-privacy-security-and-ethics-of-artificial-intelligence/

[237] http://standards.ieee.org/develop/indconn/ec/autonomous_systems.html ; see also:
https://www.ip-watch.org/2017/11/27/new-standards-projects-ieee-ethics-autonomous-intelligent-systems/

[238] https://ainowinstitute.org/AI_Now_2017_Report.pdf

[239] http://www.itu.int/en/council/cwg-internet/Pages/display-feb2016.aspx?ListItemID=13

[240] For a high-level summary, see: http://www.ip-watch.org/2016/11/30/report-ip-access-science-troubled-relationship/

[241] http://www.ictsd.org/sites/default/files/research/ceipi-ictsd_3_0.pdf . The citation is from page 14. See also pp. 84 ff. We cite from p. 85: "Copyright, originally conceived as a tool to protect the author and to provide incentives for him or her to create for the benefit of society, is nowadays more and more perceived as an instrument to the advantage of 'large, impersonal and unlovable corporations'. ... Copyright is increasingly perceived as a right to sanction and punish that prevents the free flow of information and access to knowledge or cultural participation, not as a right that has positive effects for the development of society."

Telecommunication Standardization Assembly (WTSA) that would have instructed TSAG to assess the possibility to improve the existing working methods of ITU-T, aiming to facilitate the development of ITU-T Recommendations on the basis of strong collaboration and coordination with open source projects; and to assess the possibility to increase participation and involvement of open source entities and organizations in the work of ITU-T. We note that a Resolution on open source in ITU-T was eventually adopted, but we regret that it did not include the substantive language referred to above.

Similarly, it is disappointing to note that some developed countries formally objected, at WTSA, to the adoption of certain recommendations, namely:

- Recommendation ITU-T D.52[242], Establishing and connecting regional Internet exchange points to reduce costs of international Internet connectivity, which guides regional collaboration to establish central hubs or Internet exchange points (IXPs) that enable local Internet traffic to be routed locally, saving international bandwidth and reducing the costs of international Internet connectivity.
- Recommendation ITU-T D.53[243], Universal Service, which, while recognizing the sovereign right of Member States to define and regulate their universal service/access policies, proposes general outlines to guide governments and regulators in their tasks and management functions regarding universal service funds in a globalized digital environment.
- Recommendation ITU-T D.261[244], Principles for market definition and identification of operators with significant market power, which proposes principles and guidelines to assist countries in defining and identifying significant market power (SMP) in the telecommunications sector.

3.1 Techno-imperialism

A good explanation of how a few large private companies control much of the e-commerce platforms currently in use is given at:

http://www.slate.com/articles/technology/future_tense/2016/11/countries_do_not_control_the_internet_companies_do.html

The author of the cited article had also prepared a map showing the dominance but it was not published.[245] The map is reproduced below. The author of the article provided the following explanation for the map: "It shows the Number 1 site by country as listed by Alexa.com. Red =

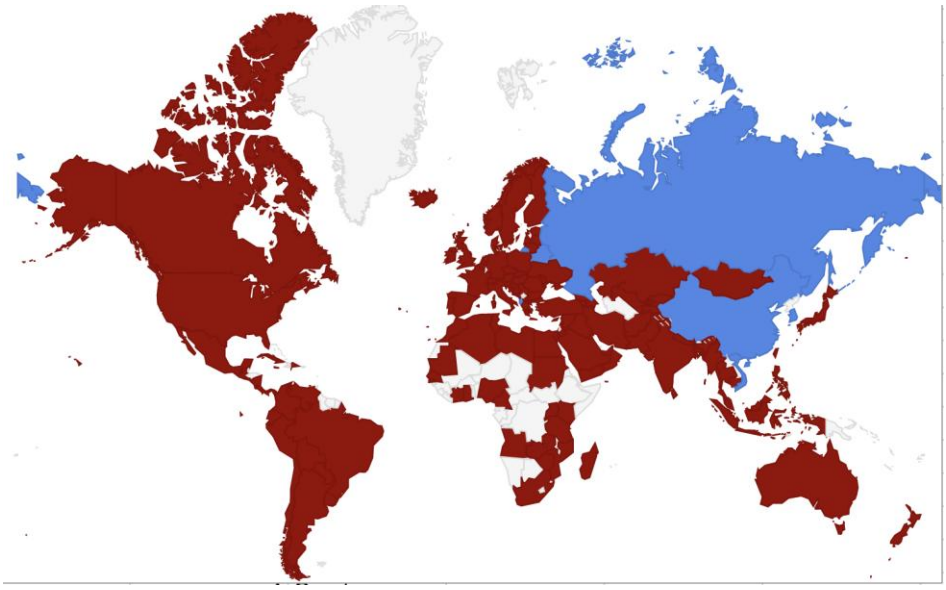
[242] The published Recommendation contains the following statement: "-The following country has expressed a reservation with respect to this Recommendation: Australia; -The following countries have expressed a reservation and will not apply this Recommendation: Canada and United States of America; -This Recommendation is not applicable to the United Kingdom."

[243] The published Recommendation contains the following statement: "-The following country has expressed a reservation with respect to this Recommendation: Australia; -The following countries have expressed a reservation and will not apply this Recommendation: Canada and United States of America; -This Recommendation is not applicable for Finland, Norway, Switzerland and Sweden; -This Recommendation is not applicable to Germany, Poland, Portugal and the United Kingdom".

[244] The published Recommendation contains the following statement: "-The following country has expressed a reservation with respect to this Recommendation: Australia; -The following countries have expressed a reservation and will not apply this Recommendation: Canada and United States of America; -This Recommendation is not applicable for Finland, Norway, Switzerland and Sweden; -This Recommendation is not applicable to Germany, Poland, Portugal and the United Kingdom".

[245] Private communication with the author of the cited article.

Google/YouTube, Blue=Other. So, we have the situation where only countries which have actively protected their home markets are not led by Google!"



4. What are good practices?

We all know the opportunity, and wish to see it realized: to make the world a better place by using e-commerce to increase social justice[246], that is the fair and just relation between the individual and society, measured in terms of the explicit and tacit terms for the distribution of wealth, opportunities for personal activity and social privileges.

In our view, the challenge is how to prevent increasing inequality[247] and the erosion of democracy[248] which are fostered by neo-liberal policies that are in reality corporatist policies that favor the profitability of a few large companies[249], in what can be referred to as techno-imperialism. As stated in section 8 of our submission to an ITU open consultation[250]:

> [Techno-imperialism is] a policy by which a group of private companies maintains or extends its control over economic and policy matters by controlling the development and use of certain technologies. Reliance on intellectual property rights such as copyrights, patents, and trade secrets are some of the means used to exercise such control.
>
> …
>
> … the interests of the technologists are conflated with the economic and policy interests of the developed countries, so that traditional colonialism is conflated with techno-imperialism.

---

[246] https://en.wikipedia.org/wiki/Social_justice

[247] http://www.newsclick.in/international/review-schiller-dan-2014-digital-depression-information-technology-and-economic-crisis

[248] http://boundary2.org/2015/04/08/the-internet-vs-democracy/

[249] http://www.boundary2.org/2015/04/dissecting-the-internet-freedom-agenda/

[250] http://www.itu.int/en/council/cwg-internet/Pages/display-feb2013.aspx?ListItemID=60

The time has come to realize that, as shown in detail above, a continuing emphasis on neo-liberal policies will not be beneficial to the world's people.

In that light, we invite all states to refrain from discussing e-commerce issues in the World Trade Organization see:

http://notforsale.mayfirst.org/en/signon/11th-wto-ministerial-letter-global-civil-society-about-agenda-wto

and:

https://www.theguardian.com/technology/2018/jan/31/data-laws-corporate-america-capitalism

Criticism of holding discussions related to the Internet in the WTO and other trade negotiation forums is not all that recent. Pages 74-75 of UNCTAD's *Information Economy Report 2017: Digitalization, Trade and Development*[251] contain the following citations:

> "Bilateral and multilateral free trade agreements can significantly affect Internet governance issues. Many, such as the Trans-Pacific Partnership Agreement, specifically address important issues such as data localization, encryption, censorship and transparency, all of which are generally regarded as forming part of the Internet governance landscape. However, they are negotiated exclusively by governments and usually in secret. At the same time, such agreements substantially benefit the Internet in a myriad of ways, such as by agreeing on rules to improve competition and market access. Further agreements such as the US-Europe Transatlantic Trade and Investment Partnership and the Trade in Services Agreement under the World Trade Organization are expected to cover similar territory. The fact that these negotiations are open only to governments has inspired protests by non-governmental actors demanding that they be informed and engaged in negotiations to allay fears that the new rules embedded in these agreements favour the interests of governments or corporations over those of other Internet users. The closed nature of the negotiations also means that the benefits governments hope to achieve may not be evident to the general public (GCIG, 2016: 78)."[252]

and

> "We recognize the considerable social and economic benefits that could flow from an international trading system that is fair, sustainable, democratic, and accountable. These goals can only be achieved through processes that ensure effective public participation. Modern trade agreements are negotiated in closed, opaque and unaccountable fora that lack democratic safeguards and are vulnerable to undue influence. These are not simply issues of principle; the secrecy prevents negotiators from having access to all points of view and excludes many stakeholders with demonstrable expertise that would be valuable to the negotiators. This is particularly notable in relation to issues that have impacts on the online and digital environment, which have been increasingly subsumed into trade agreements over the past two decades."[253]

---

[251] http://unctad.org/en/pages/PublicationWebflyer.aspx?publicationid=1872

[252] The source is the report of the Global Commission on Internet Governance, at: http://ourinternet.org/sites/default/files/inline-files/GCIG_Final%20Report%20-%20USB.pdf .

[253] The source is the Open Digital Trade Network Brussels Declaration, at: https://www.eff.org/files/2016/03/15/brussels_declaration.pdf

The cited UNCTAD report goes on to state:

> "Stakeholders have also expressed concerns about various substantive aspects of rules governing trade in the digital economy. Contentious issues include the inclusion of provisions concerning intellectual property, encryption, source codes, intermediary liability, network neutrality, spam, authentication and consumer protection."[254]

As one academic analysis puts the matter: "The new e-commerce regime is not about 'free trade' and barely about real commerce. As with the WTO's Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS), it aims to protect and entrench the oligopoly of first movers".[255] The dangers of viewing data as a commodity that should flow freely are well explained in a paper by IT for Change.[256] As two experts put the matter[257]:

> But if all the world's data flows back to a few tech powerhouses, without restrictions or taxes, this will further reinforce their monopolies, widen the privacy gap, and leave developing countries as passive consumers or data points, rather than participants in the digital economy.
>
> Those calling for liberalization use the rhetoric of creating opportunities for the poor — connecting the next billion — which sounds great, but only if we disconnect it from reality. Today, 60% world lacks even access to electricity. In the past, Spanish colonizers arrived in the Americas offering mirrors to the indigenous people in exchange for their gold. Is connectivity the "mirror" powerful actors are offering to the global poor today?
>
> Trade agreements eliminate the diversity of domestic policies and priorities, and impose costly restrictions on countries that want to address local inequalities and boost local industry. In the case of the digital economy, it will consolidate the position of few, to the detriment of the rest.

The scope of the provisions proposed in free trade negotiations is very broad and goes well beyond what the traditional scope of WTO.[258] And, as the cited scholar[259] puts the matter, citing other scholars: "We find ourselves in '. . . a system that officially claims to embrace free trade, yet still pits one political interest against another in a quest to seize protectionist rents. Powerful lobbies, such as domestic

---

[254] The cited UNCTAD report gives the following source for that statement: "Bureau Européen des Unions de Consommateurs (BEUC), Analysis of the TiSA e-commerce annex & recommendations to the negotiators, TiSA leaks, September 2016 (http://www.beuc.eu/publications/beuc-x-2016-083_lau_beucs_analysis_e-commerce_tisa_2016.pdf , accessed 1 June 2017); and EDRi's red lines on TTIP, January 2015 (https://edri.org/files/TTIP_redlines_20150112.pdf , accessed 1 June 2017). BEUC and EDRi are coalitions of 43 and 35 civil society organizations, respectively."

[255] Page 2 of Kelsey, Jane (2017) *The Risks for ASEAN of New Mega-Agreements that Promote the Wrong Model of e-Commerce*, ERIA Discussion Paper 2017-10, available at: http://www.eria.org/publications/discussion_papers/DP2017-10.html

[256] http://www.itforchange.net/sites/default/files/add/The%20grand%20myth%20of%20cross-border%20data%20flows%20in%20trade%20deals-Dec2017.pdf

[257] https://www.buzzfeed.com/burcukilic/big-tech-is-pushing-for-a-new-kind-of-free-trade

[258] See for example pp. 101 ff. of the academic analysis at: https://lawreview.law.ucdavis.edu/issues/51/1/Symposium/51-1_Burri.pdf

[259] *Op. cit.*, p. 129

producers, capture trade negotiators and replace national interests with those of their own.'" Negotiations in trade venues proceed "in a secretive, non-transparent, and non-inclusive manner."[260]

For a general discussion of the importance of transparency, see:

http://www.circleid.com/posts/20171121_transparency_the_internets_only_currency/

_____

[260] *Op. cit.*, p. 130