Contribution to the June-September 2017 Open Consultation of the ITU CWG-Internet

6 June 2017

Richard Hill[1], APIG

Summary

The time has come to recognize that OTTs are a global phenomenon and that they can be appropriately governed only by concerted global action. There is a need for global rules, which should take the form of an international legal framework. The time has come to start creating that framework, which should include a Digital Geneva Convention.

OTTs bring benefits, but they bring benefits only if people are connected. Thus, as stated in our previous contributions, there is an urgent need to reduce the cost of connectivity in developing countries. This 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.

In order to foster the continuing use of OTTs, it is necessary to improve trust and security. It is urgent to recognize that market failures are partly the cause of the current lack of security of OTTs. Steps must be taken to address the externalities arising from lack of security (entities that do not secure their systems sufficiently do not bear all the costs of security breaches), and to address information asymmetries (consumers have no way of knowing which services are sufficiently secure). At the same time, it is imperative to protect human rights, protect data privacy, protect consumers and workers (in particular against abuse by dominant platforms), curtail unnecessary and disproportionate mass surveillance, address the issue of job destruction and wealth concentration engendered by OTTs, address the ethical issues arising from automation and artificial intelligence, and deal with OTT platform dominance.

The body of the paper contains specific recommendations for each of these issues.

Background and Introduction

On 25 May 2017 Council decided that Open Consultations for the CWG-Internet would be convened on the following issue:

> Considering the rapid development of information and communications technology (ICT) which led to the advent of Internet-based services commonly known as "over-the-top" (hereafter: OTT), all stakeholders are invited to submit their inputs on the following key aspects from policy prospective:
>
> 1. What are the opportunities and implications associated with OTT?
>
> 2. What are the policy and regulatory matters associated with OTT?
>
> 3. How do the OTT players and other stakeholders offering app services contribute in aspects related security, safety and privacy of the consumer?
>
> 4. What approaches which might be considered regarding OTT to help the creation of environment in which all stakeholders are able to prosper and thrive?
>
> 5. How can OTT players and operators best cooperate at local and international level? Are there model partnership agreements that could be developed?

[1] info@apig.ch

1. What are the opportunities and implications associated with OTT?

1.1 General opportunities and implications associated with OTT

The CSTD document E/CN.16/2015/CRP.2[2], "Mapping of international Internet public policy issues", 17 April 2015, states in Chapter 9, "Concluding remarks":

> The tension between the transborder nature of the Internet, on the one hand, and predominantly national regulations that govern public policy issues pertaining to the Internet, on the other, results into challenges for the implementation of regulation. Making diverse legislation more interoperable and aligning national laws with existing international instruments helps in overcoming these challenges. At the international level, this calls for strengthened cooperation, capacity building and sharing of information and best practices.
>
> The review indicates that improvements could be made in respect of these gaps. At international level, strengthened coordination and collaboration across stakeholder groups will be critical in efforts to bridge them.

We concur with that finding and are of the view that the rule of law must exist at the international level for OTT, given that OTT services are an international phenomenon.

There is general agreement that Brexit and the election of US President Trump were driven by dissatisfaction with the results of globalization, that is, unequal distribution of the benefits[3]. Or, in other words, we strove to increase efficiency but forgot to maintain equity[4]. As The Economist Intelligence Unit puts the matter[5]:

> The parallels between the June 2016 Brexit vote and the outcome of the November 8th US election are manifold. In both cases, the electorate defied the political establishment. Both votes represented a rebellion from below against out-of-touch elites. Both were the culmination of a long-term trend of declining popular trust in government institutions, political parties and politicians. They showed that society's marginalised and forgotten voters, often working-class and blue-collar, do not share the same values as the dominant political elite and are demanding a voice of their own—and if the mainstream parties will not provide it, they will look elsewhere.

There are two solutions: stop globalizing, which is what Brexit and President Trump are about, or come up with globalized norms that ensure equity.

---

[2] http://unctad.org/meetings/en/SessionalDocuments/ecn162015crp2_en.pdf

[3] See for example the last paragraph at: http://fortune.com/2017/02/18/bill-gates-robot-taxes-automation/

[4] http://www.other-news.info/2017/02/our-collective-failure-to-reverse-inequality-is-at-the-heart-of-a-global-malaise-2/

[5] *Democracy Index 2016*, The Economist Business Intelligence Unit, page 14, at: http://pages.eiu.com/rs/783-XMC-194/images/Democracy_Index_2016.pdf

As my colleague Parminder Jeet Singh put the matter in an E-Mail (he refers to “the Internet”, but the comments are equally valid for OTT):

> The Internet is the public sphere today. It cements how the public organises and expresses. But it quite a bit more: It is a kind of a new nervous system running through the society.
>
> The Just Net Coalition, and its Delhi Declaration[6], believes, that the Internet has to be claimed as a commons and as a public good. Not a market or competitive good. It is the level playing field of the society, on which opportunities can be sought, and made good -- in a manner that is equitable for all.
>
> Internet's basic structures and layers -- whether the physical telecom layer; its key social applications, like search, social media, instant media, etc; or big data and digital intelligence, must be treated as commons, society's common property, and governed accordingly. This has to be the point of departure for Internet governance, not merely as a commonly used rhetoric, but as an actual first political principle. Things will change from then on!
>
> The original sin was when the US cast the Internet in a primarily commercial mode - with its first Internet related policy framework of "A framework for global e-commerce". One can be sure that an Internet born and nurtured in, say, a nordic country, or a developing one, would have had a different default nature. And because, with the Internet, the very playing field of the society was able to be rigged by big business, the period of coming of age of the Internet in the first decade and half of this millennium has also been of one of the fastest ever growth of inequality in the world. we must investigate this connection, and remedy it, for us to win the war against unsustainable inequality. It is vain, in these circumstances, to keep giving air to the myth of Internet's egalitarianism, it is evidently not so. Not as we have come to know it. Can it be made egalitarian. Yes, for which see above :). We must reclaim the (equal) playing field nature of the Internet.

As the UK Conservative Party put the matter in its Manifesto of 2017[7]:

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

---

[6] http://www.justnetcoalition.org/delhi-declaration

[7] See p. 83 of: https://s3.eu-west-2.amazonaws.com/manifesto2017/Manifesto2017.pdf

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

It is time to face this issue square on for what concerns OTT governance. Should we do nothing, and watch as the Internet becomes less global, or should we work towards international norms that will allow OTTs and the Internet to remain global?

And it is an OTT/Internet issue, make no mistake about it. According to Oxfam[8], eight men own as much wealth as the poorest 50% of the world's population. Of those eight[9] men, five are in ICT industries: Gates, Slim, Bezos, Zuckerberg and Ellison.

Apparently the OECD recognized the importance of international digital policy (which includes international Internet policy and thus OTT policy) when it created its Committee on Digital Economic Policy in 2014 to, inter alia, "Develop and promote a coherent policy and regulatory framework which supports competition, investment and innovation across the digital economy".[10]

Thus we urge serious consideration of the specific steps towards the second outcome – how to maintain and grow a global Internet and global OTT services– that are we are recommending. It is in this light that we propose specific recommendations in section 2 below.

1.2 Specific opportunities and implications associated with access to OTT

Users cannot access OTT unless they have affordable access to the Internet. Therefore, it is important to stress once again, that reducing the cost of connectivity must be a priority. We say "once again" because we have already made this point, and provided specific recommendations, in previous submissions to CWG-Internet.[11]

Further, it is important to address the revenue flows of OTT and to ensure that infrastructure providers are adequately compensated. We note that the mandate of Question 9[12] of ITU-T Study Group 3 includes studying the economic impact of OTT and we hope that such studies will address the issues outlined above.

---

[8] https://www.oxfam.org/en/pressroom/pressreleases/2017-01-16/just-8-men-own-same-wealth-half-world

[9] http://www.forbes.com/billionaires/list/#version:static

[10] See http://webnet.oecd.org/OECDGROUPS/Bodies/ShowBodyView.aspx?BodyID=1837&Book=True

[11] See 1.1 of http://www.itu.int/en/Lists/consultationOct2016/Attachments/24//CWG-Internet%202017.pdf

[12] https://www.itu.int/en/ITU-T/studygroups/2017-2020/03/Pages/q9.aspx

2. What are the policy and regulatory matters associated with OTT?

2.1 Evidence-based decision-making

It is generally agreed that policy decisions should be based on evidence, and that data are the best form of evidence. Today, there is a general lack of data regarding OTT matters, in particular because cost and price data are not publicly available.

In light of the fundamental importance of transparency, and of the need to have access to data in order to make evidence-based decisions, we recommend inviting all stakeholders to consider whether it would be appropriate to include a general provision on OTT cost and price transparency in a future international instrument, for example in a future version of the International Telecommunication Regulations (ITRs).

2.2 TISA and WTO e-Commerce agenda

There is no doubt that OTTs thrive and are driven by data, and that they require access to telecommunications infrastructure. According to leaked documents, question such as the free flow of data and the terms of access to foreign telecommunications infrastructure are being discussed in the context of the Trade in Services Agreements (TISA) and/or the WTO e-Commerce agenda.

In light of the fundamental importance of transparency and inclusiveness in discussions of OTT policy matters, we recommend inviting governments to refrain from discussing those matters in forums that are not transparent or inclusive. In particular we recommend inviting governments not to discuss in the context of TISA or the WTO e-Commerce agenda matters such as the free flow of data or the terms of access to foreign telecommunications infrastructure. We recommend to invite governments to discuss all matters related to OTT governance, including matters such as the free flow of date or the terms of access to foreign telecommunications infrastructure, only in forums that are transparent and inclusive, and in accordance with the roles and responsibilities outlined in paragraph 35 of the Tunis Agenda.

2.3 The economic and social value of data and its use by and for OTT services

It is obvious that personal data has great value when it is collected on a mass scale and cross-referenced.[13] Indeed, the monetization of personal data drives today's OTT/Internet services and the provision of so-called free services such as search engines.[14] Users should have greater control over the

---

[13] 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

[14] 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

ways in which their data are used.[15] 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.[16]

All states should have comprehensive data protection legislation.[17] The development of so-called "smart cities" might result in further erosion of individual control of personal data. As one journalist puts the matter[18]: "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 issues arise regarding the use of employee data by platforms (such as Uber) that provide so-called "sharing economy" services[19].

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, behaviour-predicting commercial"[20] companies.

Further, mass-collected data (so-called "big data") are increasingly being used, via computer algorithms, to make decisions that affect people's lives, such as credit rating, availability of insurance, etc.[21] The algorithms used are usually not made public so people's lives are affected by computations made

---

[15] 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

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

[17] 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

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

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

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

[21] 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

without their knowledge based on data that are often collected without their informed consent. It is important to avoid that "big data", and the algorithmic treatment of personal data, do not result in increased inequality and increased social injustice[22] which would threaten democracy.[23]

As learned scholars have put the matter[24]:

> 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.

While some national legislators and/or courts have taken steps to strengthen citizens' rights to control the way their personal data are used[25], to consider product liability issues related to data[26], and to consider the impact of big data with respect to prohibitions of discrimination in hiring[27], there does not appear to be adequate consideration of this issue at the international level.[28] Yet failure to address the

---

[22] 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

[23] 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/

[24] 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

[25] 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/

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

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

[28] 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

issue at the international level can have negative consequences, including for trade. As UNCTAD puts the matter[29]:

> 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" [30].

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[31]. 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.[32]

Regarding algorithmic use of data, what a UK parliamentary committee[33] said at the national level can be 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,

---

[29] *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

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

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

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

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

> 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.

Similarly, the recommendations of a national artificial intelligence research and development strategic plan[34] 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.
>
> **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.[35]

Consequently, we recommend to invite UNCTAD[36] and UNCITRAL to 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[37]) to make decisions, which issues include economic and legal aspects. In particular, UNCITRAL should be mandated to develop model laws, and possibly treaties, on personal

---

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

[35] 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

[36] 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

[37] 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 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

data protection[38], algorithmic transparency and accountability[39], and artificial intelligence[40]; and UNCTAD should be mandated to develop a study on the taxation of robots[41].

2.4 Takedown, filtering and blocking

An increasing number of states have implemented, or are proposing to implement, measures to restrict access to certain types of OTT content[42], e.g. incitement to violence, gambling, copyright violation, or to take measures[43] against individuals who post certain types of content.

While such measures are understandable in light of national sensitivities regarding certain types of content, the methods chosen to restrict content must not violate fundamental human rights such as freedom of speech[44], and must not have undesirable technical side-effects.

Any restrictions on access to content should be limited to what is strictly necessary and proportionate in a democratic society.

---

[38] 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 ;
and 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 ;

and the core principles found in p. 56 and 65 ff. of the cited UNCTAD study at: http://unctad.org/en/PublicationsLibrary/dtlstict2016d1_en.pdf ;

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

[39] 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

[40] 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/

[41] 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

[42] See the report at:
http://www.un.org/ga/search/view_doc.asp?symbol=A/71/373 and the press release at:
http://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=20717&LangID=E

[43] See for example
http://www.cps.gov.uk/news/latest_news/cps_publishes_new_social_media_guidance_and_launches_hate_crime_consultation/ ; and the summary article at:
https://techcrunch.com/2016/10/12/ai-accountability-needs-action-now-say-uk-mps/

[44] See the report cited above, A/71/373.

At present, there does not appear to be adequate consideration at the international level of how best to conjugate national sensitivities regarding certain types of content with human rights and technical feasibilities.

This issue is exacerbated by the fact that certain Internet service providers apply strict rules of their own to content, at times apparently limiting freedom of speech for no good reason.[45]

Since the right of the public to correspond by telecommunications is guaranteed by Article 33 of the ITU Constitution (within the limits outlined in Article 34), we recommend to invite IETF, ITU, OHCHR, and UNESCO jointly to study the issue of takedown, filtering, and blocking, which includes technical, legal, and ethical aspects.

2.5 Intermediary liability

The issue of the extent to which OTT service providers, and other intermediaries such as providers of online video content, are or should be liable for allowing access to illegal material has been addressed by many national legislators.[46]

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

We recommend to invite UNCITRAL to study the issue of intermediary liability, with a view to proposing a model law on the matter.

2.6 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.[47] This is particularly important in light of the increasing use of OTT services, which general great volumes of data. Certain states practice mass surveillance of such data that violates the right to privacy[48] (see for example A/HRC/31/64[49], A/71/373[50] A/HRC/34/60[51] and

---

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

[46] https://cyberlaw.stanford.edu/our-work/projects/world-intermediary-liability-map-wilmap ; see also 17-23 of a European Parliament Committee Report on online platforms and the digital single market, (2016/2276(INI): http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+COMPARL+PE-599.814+01+DOC+PDF+V0//EN&language=EN

[47] See for example pp. vii, 32, 106 and 133 of GCIG.

[48] 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

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

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

[51] http://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=21321&LangID=E

European Court of Justice judgment[52] ECLI:EU:C:2016:970 of 21 December 2016). As UNCTAD puts the matter[53]:

> 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[54]. 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.[55] Even a well-known business publication has recognized that privacy is a pressing issue[56].

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."[57]

It appears to us that this decision and questions[58] 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

---

[52] 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

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

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

[55] See 2 of the cited HRC Resolution

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

[5757] https://www.whitehouse.gov/the-press-office/2017/01/25/presidential-executive-order-enhancing-public-safety-interior-united

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

of [certain] diplomats"[59]). Surely there is a need to agree at the international level on an appropriate level of privacy protection for communications.

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, 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[60]). Many commentators oppose state-attempts to compromise encryption.[61] 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.[62] The cited HRC resolution calls on states not to interfere with the use of encryption.[63]

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.[64]

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. In particular, restrictions must be placed on the collection and aggregation of meta-data.[65]

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

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

---

[59] 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

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

[61] 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

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

[63] See 9 of the cited HRC Resolution

[64] See for example p. 66 of GCIG.

[65] See p. 31 of GCIG.

2.7 Internet of Things (IoT)

In the current environment, it can be expected that networked devices (the so-called Internet of Things – IoT)[66], which are a type of OTT service, will transmit data to manufacturers and service providers with little or no restrictions on the use of the data.[67] 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.[68]

Further, interconnected devices may make decisions affecting daily life,[69] 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.[70]

Increasingly, the safety of IoT devices will be affected by their security.[71] Thus, the security risks[72] posed by interconnected devices may require government actions.[73] For example, there may be a need 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[74]. In this context, it is worth considering past

---

[66] 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

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

[68] 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.

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

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

[71] http://www.cl.cam.ac.uk/~rja14/Papers/weis2017.pdf

[72] 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

[73] 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

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

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[75], 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[76] (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.[77] As one security manager put the matter[78]: "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 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

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[79]). The studies should take into account Recommendation ITU-T Y.3013: Socio-economic assessment of future networks by tussle analysis[80].

---

[75] 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

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

[77] 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

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

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

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

2.8 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.[81] This issue is particularly important for OTT services. 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.[82] 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.[83] The cost of the attack was borne by the end-users, not by the software manufacturer.

As the Global Internet Report 2016 of the Internet Society puts the matter[84]:

> 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[85] that affected a large number of users and many hospitals.

As the European Union Agency for Network and Information Security (ENISA) puts the matter[86]: "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 noted above, the externalities arising from lack of security are exacerbated by the Internet of Things (IoT)[87]. As a well known security expert puts the matter[88]: "Security engineers are working on

---

[81] 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/

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

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

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

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

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

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

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

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.[89]

Some national authorities are taking some measures.[90] In particular, the President of the USA issued an Executive Order[91] 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[92] 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.

---

[89] https://www.cigionline.org/internet-survey

[90] 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

[91] 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

[92] 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

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.

Further, as stated by the President of a leading software company (Microsoft)[93]:

> 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[94], the official presenting the cited US Executive Order[95] stated:

---

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

> ... 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.
>
> ...
>
> ... [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[96] in mid-May 2017, Microsoft reinforced its call for action, stating[97]:

> 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.

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 particular on the Internet, in times of peace, and to consider whether to

---

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

[95] 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

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

[97] https://blogs.microsoft.com/on-the-issues/2017/05/14/need-urgent-collective-action-keep-people-safe-online-lessons-last-weeks-cyberattack/#sm.00017arazqit2faipqq2lyngzmxx4

develop a new treaty, or whether to invite the ITU to integrate such norms into its own instruments, for example the International Telecommunication Regulations.

2.9 Ethical issues of networked automation, including driverless cars

One component of OTT is that 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.[98] 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[99].

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." [100] See also the discussion of algorithmic data processing and artificial intelligence presented under item 1 above.

At present, some action have been proposed at the national level[101], 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, including driverless cars, which include ethical and legal aspects.[102] 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.[103]

2.10 How to deal with induced job destruction and wealth concentration

Scholars have documented the reduction in employment that has already been caused by OTT services and automation. It is likely that this trend will be reinforced in the future.[104] Even if new jobs are

---

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

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

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

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

[102] 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.

[103] http://standards.ieee.org/develop/indconn/ec/autonomous_systems.html

[104] http://robertmcchesney.org/2016/03/01/people-get-ready-the-fight-against-a-jobless-economy-and-a-citizenless-democracy/ and

created as old jobs are eliminated, the qualifications for the new jobs are not the same as the qualifications for the old jobs.[105] And artificial intelligence can even result in the elimination of high-skilled jobs[106], including creation of software[107]. These developments, including the so-called sharing economy, pose policy and regulatory challenges.[108]

Further, it has been observed that income inequality[109] is increasing in most countries, due at least in part to the deployment of ICTs[110]. 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[111]. Indeed, it has been 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

---

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 .
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

[105] 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

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

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

[108] 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

[109] See for example https://www.oxfam.org/en/research/working-few and
https://www.oxfam.org/en/research/economy-99

[110] 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

[111] 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. 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 .

goals may erode social justice.[112] Further, the algorithms that are increasingly used to automate decisions such as granting home loans may perpetuate or even increase inequality and social injustice.[113]

At present, there does not appear to be adequate consideration of these issues at the international level, even if ILO[114] 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.

2.11 How to deal with platform dominance

It is an observed fact that, for certain specific OTT services (e.g. Internet searches, social networks, online book sales, online hotel reservations) one particular provider becomes dominant. If the dominance is due to a better service offer, then market forces are at work and there is no need for regulatory intervention.

But if the dominance is due to economies of scale and network effects, then a situation akin to a natural monopoly[115] might arise, there might be abuse of dominant market power[116], and regulatory intervention is required[117]. For example, platforms might abusively use personal data to set high prices for goods for certain customers.[118]

---

[112] 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

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

[114] http://www.other-news.info/2017/04/humanity-and-social-justice-a-must-for-the-future-of-work-ryder/

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

[116] 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 ; 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 .
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

[117] A forceful and well-reasoned call for regulation has been given by *The Economist*, see:

Appropriate regulatory intervention might be different from that arising under competition or anti-trust policies.[119] As one commentator puts the matter[120] (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 noted above, the dominance of certain platforms[121] raises issues related to freedom of speech, because some platforms apply strict rules of their own to censor certain types of content[122], and, for

---

http://www.economist.com/news/leaders/21721656-data-economy-demands-new-approach-antitrust-rules-worlds-most-valuable-resource ; 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/ .
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.

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

[119] https://www.competitionpolicyinternational.com/let-the-right-one-win-policy-lessons-from-the-new-economics-of-platforms/

[120] 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

[121] 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/

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

many users, there are no real alternatives to dominant platforms[123]; and some workers might also face limited choices due to dominant platforms[124].

As *The Economist* puts the matter[125]:

> "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 content delivery networks where the rules are written by a handful of content owners, ignoring any concept of national sovereignty.[126]

And, citing *The Economist* again[127]:

> 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[128]:

> 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

---

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

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

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

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

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

[128] 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

> 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.

Measures to ensure accountability may be needed with respect to labor-relation issues, and not with respect to users and consumers.[129]

National authorities in a number of countries have undertaken investigations,[130] and even imposed measures,[131] in specific cases. And at least one influential member of a national parliament has expressed concern about some major Internet companies "because they control essential tech platforms that other, smaller companies depend upon for survival."[132] The Legal Affairs Committee of the European Parliament adopted an Opinion in May 2017 that, among other provisions[133]:

> 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).[134]

However, it does not appear that there is an adequate platform for exchanging national experiences regarding such matters.[135]

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.[136]

---

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

[130] 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

[131] See for example http://www.autoritedelaconcurrence.fr/user/standard.php?id_rub=606&id_article=2534

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

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

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

[135] 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

We recommend to invite UNCTAD to study the economic and market issues related to platform dominance, and to facilitate the exchange of information on national and regional experiences, and that the ILO be mandated to study the worker protection issues related to platform dominance and the so-called "sharing economy".

Further, dominant search platforms may, inadvertently or deliberately, influence election results, which may pose an issue for democracy.[137]

We recommend to invite the Inter-Parliamentary Union (IPU) and the UN HCHR to study the potential effects of platform dominance on elections and democracy.

2.12 How to deal with embedded software

More and more OTT services and devices used in ordinary life, including in particular automobiles, depend more and more on software. Software is protected by copyright law. Thus users who buy a device have increasingly less control over the device, because they cannot change the software controls the device. This raises significant policy issues.[138] In fact, attempts to change the software may be criminal acts in some countries.

This situation may result in a significant shift of market power away from consumers, thus reducing competition. Indeed, a respected computer scientist has called for the establishment, at the national level of an "algorithm safety board"[139]. At present, there does not appear to be adequate consideration of these issues at the international level.

We recommend to invite UNCTAD and WIPO to study the issues related to embedded software, which include economic and legal issues.

---

[136] 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 .
A more general discussion of various issues arising out of platform dominance is at:
http://www.alainet.org/en/articulo/181307

[137] 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
for a possible impact on free speech, see:
http://www.globalresearch.ca/google-corporate-press-launch-attack-on-alternative-media/5557677 .

[138] http://copyright.gov/policy/software/

[139] http://www.techworld.com/big-data/pioneering-computer-scientist-calls-for-national-algorithms-safety-board-3659664/

3. How do the OTT players and other stakeholders offering app services contribute in aspects related security, safety and privacy of the consumer?

As noted above, the use of data by OTT players and mass surveillance practiced by some governments threatens the privacy of consumers. Further, the security and safety of consumers are threatened by the current OTT governance regime, which does not take into account adequately the market failures created by security externalities and information asymmetries.

4. What approaches which might be considered regarding OTT to help the creation of environment in which all stakeholders are able to prosper and thrive?

See the specific recommendations in section 2 above.

5. How can OTT players and operators best cooperate at local and international level? Are there model partnership agreements that could be developed?

See the specific recommendations in section 2 above.

_____