# UNITED NATIONS COMMISSION ON SCIENCE AND TECHNOLOGY FOR DEVELOPMENT

## Working Group on Enhanced Cooperation

## Revised recommendations submitted in preparation for the 4th WGEC meeting

Submitted by

**Richard Hill**

**International Internet Public Policy Issues: Proposed Recommendations**

Richard Hill
Association for Proper Internet Governance[1]
28 August 2017

## A. Introduction

This submission addresses the question: "2. Taking into consideration the work of the previous WGEC and the Tunis Agenda, particularly paragraphs 69-71, what kind of recommendations should we consider?"

It presents revised versions of recommendations presented previously. The revisions are intended to accommodate comments made during discussions.

This submission contains the following sections:

A. Introduction

B. Scope of Internet Governance

C. Importance of International Policies

D. Specific Recommendations

## B. Scope of Internet Governance

As a preliminary matter, we discuss what is in the scope of "Internet governance".

The Tunis Agenda states:

> **33.** We take note of the WGIG's report that has endeavoured to develop a working definition of Internet governance. It has helped identify a number of public policy issues that are relevant to Internet governance. The report has also enhanced our understanding of the respective roles and responsibilities of governments, intergovernmental and international organizations and other forums as well as the private sector and civil society from both developing and developed countries.
>
> **34.** A working definition of Internet governance is the development and application by governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet.
>
> …

[1] http://www.apig.ch

> **58.** We recognize that Internet governance includes more than Internet naming and addressing. It also includes other significant public policy issues such as, inter alia, critical Internet resources, the security and safety of the Internet, and developmental aspects and issues pertaining to the use of the Internet.
>
> **59.** We recognize that Internet governance includes social, economic and technical issues including affordability, reliability and quality of service.
>
> **60.** We further recognize that there are many cross-cutting international public policy issues that require attention and are not adequately addressed by the current mechanisms.

Thus the scope of Internet governance encompasses the evolution and use of "the Internet". Various definitions of the term "the Internet" are in use[2]. It appears to us that a definition which corresponds well to what is commonly meant by "the Internet", and which is consistent with the provisions of the Tunis Agenda, would be similar to the one adopted in 1995 by the US Federal Networking Council[3]:

> [The Internet is] the global information system that:
>
> (i) is logically linked together by a globally unique address space based on the Internet Protocol (IP) or its subsequent extensions/follow-ons;
>
> (ii) is able to support communications using the Transmission Control Protocol/Internet Protocol (TCP/IP) suite or its subsequent extensions/follow-ons, and/or other IP-compatible protocols; and
>
> (iii) provides, uses or makes accessible, either publicly or privately, high level services layered on the communications and related infrastructure described herein.

This is an extremely broad definition, since it encompasses the applications that run on top of the TCP/IP protocol as well as the hardware that is interconnected by that protocol.

The Tunis Agenda visibly adopted, albeit implicitly, a very expansive view of what is included in Internet governance (and by implication of what is included in "the Internet"), because the following specific issues are mentioned in paragraphs 38-54 and 63-64 of the Tunis Agenda:

- Resource management
- Confidence and security
- Trust framework
- Protection of personal information, privacy and data
- Cybercrime
- Spam

---

[2] See section 3 of Hill, R. (2014), "The Internet, its governance, and the multi-stakeholder model", *Info*, vol. 16. no. 2, March 2014 . A pre-published version of that section is at: http://www.apig.ch/Internet%202-definition.doc

[3] See footnote xv in Kahn, R. E. and Cerf, V. G. (1999), **"**What Is The Internet (And What Makes It Work)", December, available at: http://www.cnri.reston.va.us/what_is_internet.html

- Freedom to seek, receive, impart and use information
- Preventing abusive use
- Countering terrorism
- Continuity and stability
- Right to access information
- Consumer protection in the context of e-business
- E-government
- Bridging the digital divide
- International interconnection costs
- Capacity building
- Technology/know-how transfer
- Multilingualism
- Appropriate software solutions
- ICT education and training
- Enabling environment
- ccTLDs
- gTLDs

All of the recommendations below relate to one of the issues listed above.

The previous Working Group on Enhanced Cooperation (WGEG) also implicitly adopted a very expansive view of what is included in Internet governance, see the table of contents of document E/CN.16/2015/CRP.2[4], Mapping of international Internet public policy issues, 17 April 2015. And the list of international Internet-related public policy matters to be discussed in ITU's Council Working Group on International Internet-related Public Policy Issues – which list which was established in accordance with decisions of ITU membership at the Plenipotentiary Conference, Council and world conferences – is comparably broad, see Annex 1 of ITU Council Resolution 1305 of 2009.

**C. Importance of International Policies**

The cited document "Mapping of international Internet public policy issues" 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.

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

> 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 the Internet, given that the Internet is 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[5]. Even the July G20 Leaders' Declaration acknowledges that "globalization has created challenges and its benefits have not been shared widely enough"[6]. Or, in other words, we strove to increase efficiency but forgot to maintain equity[7]. As The Economist Intelligence Unit puts the matter[8]:

> 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.

As my colleague Parminder Jeet Singh put the matter in an E-Mail:

> 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[9], 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.

---

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

[6] Page 2 of https://www.g20.org/gipfeldokumente/G20-leaders-declaration.pdf . The same point is made on p. 3: "We recognise that the benefits of international trade and investment have not been shared widely enough. We need to better enable our people to seize the opportunities and benefits of economic globalisation."

[7] http://www.other-news.info/2017/02/our-collective-failure-to-reverse-inequality-is-at-the-heart-of-a-global-malaise-2/ and http://www.other-news.info/2017/06/myths-of-globalization-noam-chomsky-and-ha-joon-chang-in-conversation/ and paragraph 4.6.2 of http://congress.world-psi.org/wp-content/uploads/2017/05/EN-PoA-final-May-2017.pdf ; for an economic explanation in terms of ICTs, see: https://www.technologyreview.com/s/608095/it-pays-to-be-smart/

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

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

> 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[10]:

> 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.
>
> 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.

We, WGEC, have an opportunity to face this issue square on for what concerns Internet governance. Should we do nothing, and watch as the Internet becomes less global, or should we work towards international norms that will allow the Internet to remain global? As a senior official of the European Commission put the matter regarding the future of the Internet[11]: "We must address the real concerns of citizens, such as lack of trust, choice and respect and worst of all lock-in effects."

---

[10] See p. 83 of: https://s3.eu-west-2.amazonaws.com/manifesto2017/Manifesto2017.pdf
[11] https://ec.europa.eu/digital-single-market/en/blog/what-future-internet

And gobal issues are Internet issues, make no mistake about it. According to Oxfam[12], eight men own as much wealth as the poorest 50% of the world's population. Of those eight[13] 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) 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".[14]

Thus we urge serious consideration of the specific steps towards the second outcome – how to maintain and grow a global Internet – that are we are recommending. It is in this light that we propose specific recommendations on how to further implement enhanced cooperation as envisioned in the Tunis Agenda.

**D. Specific Recommendations**

Specific proposed recommendations are shown as text in boxes below.

These recommendations are revised versions of the recommendations submitted previously. For convenience, the recommendations are numbered using the same numbers as in the compilation (dated 26 April 2017) of recommendations discussed at the third meeting of WGEG. The recommendations below abrogate and replace the recommendations that we submitted previously.

The recommendations that were already introduced and discussed at the third meeting are identified by the suffix "D" after the recommendation number.

We note that many sections of the cited "Mapping of international Internet public policy issues" identify areas where further study would be appropriate, in particular:

2.7 Net neutrality

2.8 Cloud

2.10 Internet of Things (IoT)

3.1 Cybersecurity

3.2 Cybercrime

3.4 Cyber conflict

3.6 Encryption

[12] https://www.oxfam.org/en/pressroom/pressreleases/2017-01-16/just-8-men-own-same-wealth-half-world
[13] http://www.forbes.com/billionaires/list/#version:static
[14] See http://webnet.oecd.org/OECDGROUPS/Bodies/ShowBodyView.aspx?BodyID=1837&Book=True

3.7 Spam

4.1 Freedom of expression

4.2 Privacy and data protection

5.3 Copyright

5.5 Labour law

5.6 Intermediaries

**Recommendation 38**

We concur with the findings of the document E/CN.16/2015/CRP.2, Mapping of international Internet public policy issues, 17 April 2015, and propose to recommend that all the recommendations for further study in the cited document be endorsed.

**Recommendations 39 and 40**

These are not specific recommendations and they are hereby withdrawn.

Discussions that are planned to take place in the context of the World Trade Organization (WTO) could have significant implications for Internet governance[15]. As two experts put the matter[16]:

> One must wonder whether this [negotiations in WTO] will be an opportunity to foster digital rights or leave us with even lower standards and a concentrated, quasi-monopolistic market benefiting from public infrastructure? The rhetoric of opportunities for the excluded – connecting the next billion – sounds great, but only if we disconnect it from the current realities of the global economy, where trade deals push for deregulation, for lower standards of protection for the data and privacy of citizens, where aggressive copyright enforcement risks the security of devices, and when distributing the benefits, where big monopolies, tech giants (so called GAFA) based mostly in the US, to put it bluntly, take them all.
>
> …

[15] See for example WTO documents JOB/SERV/248/Rev.2 and TN/S/W/64. See in this context our submission to the ITU Council Working Group on Internet-related Public Policy Issues, at: http://www.itu.int/en/council/cwg-internet/Pages/display-June2017.aspx?ListItemID=5 . For an overall analysis of the WTO proposals, see: http://www.huffingtonpost.com/entry/state-of-play-in-the-wto-toward-the-11th-ministerial_us_5951365ae4b0f078efd98399 ; see also: http://www.itu.int/en/council/cwg-internet/Pages/display-June2017.aspx?ListItemID=7

[16] https://www.opendemocracy.net/digitaliberties/renata-avila-burcu-kilic/new-digital-trade-agenda-are-we-giving-away-internet

> Never before has a trade negotiation had such a limited number of beneficiaries. Make no mistake, what will be discussed there, with the South arriving unprepared, will affect each and every space, from government to health, from development to innovation going well beyond just trade. Data is the new oil – and we need to start organising ourselves for the fourth industrial revolution. The data lords, those who have the computational power to develop superior products and services from machine learning and artificial intelligence, want to make sure that no domestic regulation, no competition laws, privacy or consumer protection would interfere with their plans.
>
> …
>
> Disguised as support for access and affordability, they [dominant Internet data-driven companies] want everyone to connect as fast as they can. Pretending to offer opportunities to grow, they want to deploy and concentrate their platforms, systems and content everywhere in the world. Enforcement measures will be coded in technology, borders for data extraction will be blurred, the ability to regulate and protect the data of citizens will be disputed by supranational courts, as local industries cannot compete and local jobs soar. If we are not vigilant, we will rapidly consolidate this digital colonisation, a neo-feudal regime where all the rules are dictated by the technology giants, to be obeyed by the rest of us.

**Recommendation 21D**

In light of the fundamental importance of transparency and inclusiveness in discussions of international Internet 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 the Trade in Services Agreements (TISA) 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 Internet 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.

**Recommendation 22D**

In light of the fundamental importance of transparency, we recommend inviting all entities involved in Internet governance discussions, including civil society entities, to be transparent with respect to their funding sources.

**Recommendation 23**

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 price transparency in a future international instrument, for example in a future version of the International Telecommunication Regulations (ITRs).

Further, we have indentified some additional areas where further studies would be appropriate. Consequently, we submit specific proposals regarding the following international Internet public policy issues that require more study than is taking place at present:

1. The economic and social value of data and its processing
2. Takedown, filtering and blocking
3. Intermediary liability
4. Privacy, encryption and prevention of inappropriate mass surveillance
5. How to deal with the Internet of Things (IoT)
6. Externalities arising from lack of security and how to internalize such externalities
7. Ethical issues of networked automation, including driverless cars
8. How to deal with the job destruction and wealth concentration induced by ICTs in general and the Internet in particular
9. How to deal with platform dominance
10. How to deal with the increasing importance of embedded software
11. Issues related to ccTLDs and gTLDs
12. Roles and responsibilities

**1. 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.[17] Indeed, the monetization of personal data drives today's Internet services and the provision of so-called free services such as search engines.[18] These developments have significant

[17] 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

[18] 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

implications, in particular for developing countries.[19] Users should have greater control over the ways in which their data are used.[20] 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.[21] 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[22].

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."[23]

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"[24] 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[25].

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.[26]

All states should have comprehensive data protection legislation.[27] The development of so-called "smart cities" might result in further erosion of individual control of personal data. As one journalist

---

[19] http://twn.my/title2/resurgence/2017/319-320/cover03.htm

[20] 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

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

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

[23] 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

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

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

[26] 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

puts the matter[28]: "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[29].

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"[30] companies.

Further, mass-collected data (so-called "big data"[31]) are increasingly being used, via computer algorithms, to make decisions that affect people's lives, such as credit rating, availability of insurance, etc.[32] 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. It is important to avoid that "big data", and the algorithmic treatment of personal data, do not result in increased inequality[33] and increased social injustice[34] which would threaten democracy.[35]

---

[27] 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

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

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

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

[31] 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

[32] 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

[33] https://inequality.org/facts/income-inequality/

[34] 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

[35] 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/

As learned scholars have put the matter[36]:

> 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."[37]

Control of large amounts of data may lead to dominant positions that impeded competition[38]. 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."[39]

While some national legislators and/or courts have taken steps to strengthen citizens' rights to control the way their personal data are used[40], to consider product liability issues related to data[41], and to consider the impact of big data with respect to prohibitions of discrimination in hiring[42], there does not appear to be adequate consideration of this issue at the international level.[43] Yet failure to address the

---

[36] 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

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

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

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

[40] 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/

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

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

[43] 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

issue at the international level can have negative consequences, including for trade. As UNCTAD puts the matter[44]:

> 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" [45].

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[46]. 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.[47]

Regarding algorithmic use of data, what a UK parliamentary committee[48] 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

---

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

[44] *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

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

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

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

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

> 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.

Similarly, the recommendations of a national artificial intelligence research and development strategic plan[49] 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.[50]

And experts speaking at a conference[51] on Artificial Intelligence hosted by the ITU raised many of the issues raised in this paper[52], 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[53], as did a report by the UK Royal Society[54]. An academic treatment of the issues is given in Wachter, S., Mittelstadt, B., and Floridi, L.

---

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

[50] 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

[51] http://www.itu.int/en/ITU-T/AI/Pages/201706-default.aspx

[52] 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/

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

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

(2017) "Transparent, explainable, and accountable AI for robotics", *Science Robotics,* 31 May 2017, Vol. 2, Issue 6, eaan6080, DOI: 10.1126/scirobotics.aan6080[55].

**Recommendation 2**

We recommend to invite UNCTAD[56] 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[57]) 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 data protection[58], algorithmic transparency and accountability[59], and artificial intelligence[60]; UNCTAD should be mandated to develop a study on the taxation of robots[61]; and the UN Conference on Disarmament should consider taking measures with respect to lethal autonomous weapons[62].

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

[56] 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

[57] 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 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/ ; 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

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

[59] 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

[60] 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/

[61] 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

[62] A Governmental Group of Experts on this topic has been created, see: https://www.unog.ch/80256EE600585943/(httpPages)/F027DAA4966EB9C7C12580CD0039D7B5?OpenDocument

**2. Takedown, filtering and blocking**

An increasing number of states have implemented, or are proposing to implement, measures to restrict access to certain types of Internet content[63], e.g. incitement to violence, gambling, copyright violation, or to take measures[64] 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[65], 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. [66]

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. [67]

**Recommendation 3**

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.

**3. Intermediary liability**

The issue of the extent to which Internet 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.[68]

---

[63] 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

[64] 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/

[65] See the report cited above, A/71/373 and paragraph 49 of A/HRC/35/22 at http://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/35/22

[66] See in this respect the 30 March 2017 Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, document A/HRC/35/22. At http://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/35/22

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

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

**Recommendation 4**

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

**4. 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.[69] Certain states practice mass surveillance that violates the right to privacy[70] (see for example A/HRC/31/64[71], A/71/373[72], A/HRC/34/60[73] and European Court of Justice judgment[74] 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.[75] As UNCTAD puts the matter[76]:

> 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.

---

[68] 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

[69] 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

[70] 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

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

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

[73] 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**.

[74] 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

[75] 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

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

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[77]. 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.[78] Even a well-known business publication has recognized that privacy is a pressing issue[79]. 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.[80]

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."[81]

It appears to us that this decision and questions[82] 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" [83]). 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[84]). Many commentators oppose state-attempts to compromise encryption.[85] 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

---

[77] http://www.un.org/ga/search/view_doc.asp?symbol=A/HRC/34/L.7/Rev.1
[78] See 2 of the cited HRC Resolution
[79] http://www.economist.com/news/briefing/21721634-how-it-shaping-up-data-giving-rise-new-economy
[80] https://www.internetsociety.org/doc/issue-paper-asia-pacific-bureau-%E2%80%93-online-privacy
[8181] https://www.whitehouse.gov/the-press-office/2017/01/25/presidential-executive-order-enhancing-public-safety-interior-united
[82] See for example: http://www.sophieintveld.eu/letter-to-eu-commission-what-impact-has-trump-decisions-on-privacy-shield-and-umbrella-agreement/
[83] 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
[84] https://documents-dds-ny.un.org/doc/UNDOC/GEN/G15/095/85/PDF/G1509585.pdf?OpenElement
[85] 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

on freedom of expression and the right to privacy.[86] The cited HRC resolution calls on states not to interfere with the use of encryption.[87]

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.[88]

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[89]. In particular, restrictions must be placed on the collection and aggregation of meta-data.[90]

There does not appear to be adequate consideration of the issues outlined above at the international level.[91]

**Recommendation 5**

We recommend to invite IETF, ISOC, ITU, and OHCHR[92] to study the issues of privacy, encryption and prevention of inappropriate mass surveillance, which include technical, user education, and legal aspects.

**5. Internet of Things (IoT)**

In the current environment, it can be expected that networked devices (the so-called Internet of Things – IoT)[93] will transmit data to manufacturers and service providers with little or no restrictions on the use of the data. [94] 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.

[86] See in particular pp. 54 ff. The Report is at: http://unesdoc.unesco.org/images/0024/002465/246527e.pdf
[87] See 9 of the cited HRC Resolution
[88] See for example p. 66 of GCIG.
[89] For a specific proposal, see the last page of the proposals at: https://justnetcoalition.org/sites/default/files/HCHR_report_final.pdf
[90] See p. 31 of GCIG.
[91] See paragraph 46 of http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session34/Documents/A_HRC_34_60_EN.docx
[92] 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
[93] 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
[94] See https://www.theguardian.com/technology/2015/jul/15/internet-of-things-mass-surveillance and the articles it references.

Such uses of data that are collected automatically for a specific purpose could have wide-reaching and unforeseen consequences.[95]

Further, interconnected devices may make decisions affecting daily life,[96] 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.[97]

Increasingly, the safety of IoT devices will be affected by their security.[98] Thus, the security risks[99] posed by interconnected devices may require government actions.[100] 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[101]. 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[102], 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".

---

[95] 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.

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

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

[98] 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

[99] 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

[100] 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

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

[102] 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

Since IoT products will be interconnected, at least to some degree, chaos can ensue if the products are not sufficiently secure[103] (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.[104] As one security manager put the matter[105]: "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

In the US, a law[106] has been proposed to that would set minimum security standards for the government's purchase and use of a broad range IoT devices.[107]

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.

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

**Recommendation 6**

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[108]). The studies should take into account Recommendation ITU-T Y.3013: Socio-economic assessment of future networks by tussle analysis[109] as well as work in other bodes, in particular IEEE[110].

---

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

[104] 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

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

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

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

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

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

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

**6. 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.[111] 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.[112] 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.[113] 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[114]:

> 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[115] that affected a large number of users and many hospitals.

As the European Union Agency for Network and Information Security (ENISA) puts the matter[116]: "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)[117]. As a well known security expert puts the matter[118]: "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

---

[111] 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/

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

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

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

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

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

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

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

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.[119]

Some national authorities are taking some measures.[120] In particular, the President of the USA issued an Executive Order[121] 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[122] 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 for international regulations for digital markets, and in particular for international standards and rules for security.[123]

---

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

[120] 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

[121] 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

[122] 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

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

**Recommendation 7**

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)[124]:

> 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.

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

In a press conference on 11 May 2017[125], the official presenting the cited US Executive Order[126] 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.
>
> ...
>
> ... [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[127] in mid-May 2017, Microsoft reinforced its call for action, stating[128]:

> 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.[129]

---

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

[126] 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

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

[128] 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/

**Recommendation 20**

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

**7. Ethical issues of networked automation, including driverless cars**

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.[130] 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[131].

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." [132] 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[133], but there does not appear to be adequate consideration of these issues at the international level.

**Recommendation 8**

We recommend to invite UNESCO and UNICTRAL to study the ethical issues of networked automation, including driverless cars, which include ethical and legal aspects.[134] As a starting point, the study should consider the IEEE Global Initiative for Ethical Considerations in Artificial Intelligence and Autonomous

---

[129] 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

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

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

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

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

[134] 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/

Systems. *Ethically Aligned Design: A Vision For Prioritizing Wellbeing With Artificial Intelligence And Autonomous Systems*, Version 1. IEEE, 2016.[135]

**8. How to deal with induced job destruction and wealth concentration**

Scholars have documented the reduction in employment that has already been caused by automation[136]. It is likely that this trend will be reinforced in the future.[137] 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.[138] And artificial intelligence can even result in the elimination of high-skilled jobs[139], including creation of software[140]. These developments, including the so-called sharing economy, pose policy and regulatory challenges[141], in particular for developing countries[142].

---

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

[136] 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/

[137] 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 .
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

[138] 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

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

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

[141] 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 .
The legal issues are well summarized in the 4 April 2017 report of the International Bar Association "Artifical Intelligence and Robotics and Their Impact on the Workplace", available at: https://www.ibanet.org/Article/NewDetail.aspx?ArticleUid=012a3473-007f-4519-827c-7da56d7e3509

Further, it has been observed that income inequality[143] is increasing in most countries, due at least in part to the deployment of ICTs[144]. 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[145]. 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 goals may erode social justice.[146] Further, the algorithms that are increasingly used to automate decisions such as granting home loans may perpetuate or even increase inequality and social injustice.[147]

At present, there does not appear to be adequate consideration of these issues at the international level, even if ILO[148] has recently started to address some of the issues.

**Recommendation 9**

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.

**9. 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[149]. If the dominance is

---

[142] 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

[143] 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/

[144] 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

[145] 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 .

[146] 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

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

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

[149] 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/

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[150], then a situation akin to a natural monopoly[151] might arise, there might be abuse of dominant market power[152], and regulatory intervention is required[153]. For example, platforms might abusively use personal data to set high prices for goods for certain customers,[154] or a dominant search engine might provide search results that favor certain retail sites[155], or a dominant national provider might impede the operation of an international competitor[156].

Further, as already noted, control of large amounts of data may lead to dominant positions that impeded competition[157]. As a learned commentator puts the matter[158]:

---

[150] 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/

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

[152] 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

[153] 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 ; 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.

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

[155] 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

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

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

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

> 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 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 competition or anti-trust policies.[159] As one commentator puts the matter[160] (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[161] raises issues related to freedom of speech, because some platforms apply strict rules of their own to censor certain types of content[162], and, for many users, there are no real alternatives to dominant platforms[163]; and some workers might also face limited choices due to dominant platforms[164].

As *The Economist* puts the matter[165]:

---

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

[160] 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

[161] 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/

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

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

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

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

> "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.[166]

And, citing *The Economist* again[167]:

> 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[168]:

> 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.

Measures to ensure accountability may be needed with respect to labor-relation issues, and not with respect to users and consumers.[169]

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."[170]

---

[166] https://disruptive.asia/transit-dead-content-literally-rules/
[167] http://www.economist.com/news/briefing/21721634-how-it-shaping-up-data-giving-rise-new-economy
[168] 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
[169] https://www.nytimes.com/interactive/2017/04/02/technology/uber-drivers-psychological-tricks.html?_r=2
[170] https://www.theguardian.com/commentisfree/2016/dec/04/data-populists-must-seize-information-for-benefit-of-all-evgeny-morozov

National authorities in a number of countries have undertaken investigations,[171] and even imposed measures,[172] 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."[173] The Legal Affairs Committee of the European Parliament adopted an Opinion in May 2017 that, among other provisions[174]:

> 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).[175]

However, it does not appear that there is an adequate platform for exchanging national experiences regarding such matters.[176]

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.[177]

**Recommendation 10**

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

---

[171] 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

[172] 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

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

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

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

[176] 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

[177] 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

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.[178]

**Recommendation 11**

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.

**10. How to deal with embedded software**

More and more 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.[179] 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"[180]. At present, there does not appear to be adequate consideration of these issues at the international level.

**Recommendation 12**

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

[178] 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 .

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

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

**11. Issues related to ccTLDs and gTLDs**

The Tunis Agenda states:

> **68.** We recognize that all governments should have an equal role and responsibility for international Internet governance and for ensuring the stability, security and continuity of the Internet. **We also recognize** the need for development of public policy by governments in consultation with all stakeholders.
>
> **69.** We further recognize the need for enhanced cooperation in the future, to enable governments, on an equal footing, to carry out their roles and responsibilities, in international public policy issues pertaining to the Internet, but not in the day-to-day technical and operational matters, that do not impact on international public policy issues.

As noted above, issues related to ccTLDs and gTLD are squarely within the mandate of enhanced cooperation. Policies relating to ccTLDs and gTLDs are developed and maintained by the Internet Corporation for Assigned Names and Numbers.

**11.1 Equal treatment for ccTLDs**

On 6 June 2016, as part of the IANA transition process, the Internet Corporation for Assigned Names and Numbers (ICANN) and the US National Telecommunications and Information Administration (NTIA) exchanged letters[181]. In its letter, ICANN confirmed that it will not take any action to re-delegate the top-level domain names ".edu", ".gov", ".mil", and ".us" (which are administered by the US Government) without first obtaining express written approval from NTIA.

This exchange of letters is presumably a binding contract between ICANN and the US government. That is, ICANN cannot take actions regarding these domain names without the agreement of the US government.

The top-level domain name ".us" is a country code domain name, that is, a ccTLD.

According to the Principles and Guidelines for the Delegation and Administration of Country Code Top Level Domains[182] of ICANN's Government Advisory Committee (GAC), approved on 5 April 2005 (emphasis added): "4.1.2. Every country or distinct economy with a government or public authority recognised in accordance with article 3.8 above should be able to ask for its appropriate country code to be represented as a ccTLD in the DNS and to designate the Registry for the ccTLD concerned."

The term "should" is used elsewhere in the cited GAC Principles and Guidelines.

Thus the cited GAC Principles and Guidelines do not create a binding obligation for ICANN not to take actions regarding ccTLDs without the agreement of the concerned government.

---

[181] https://www.ntia.doc.gov/page/exchange-letters-us-government-administered-tlds

[182] https://gacweb.icann.org/display/GACADV/ccTLDs?preview=/28278844/28475457/ccTLD_Principles_0.pdf

In line with the principles of equal footing and equal roles and responsibilities of all governments enunciated in the Tunis Agenda, all government should be treated equally with respect to their ccTLD.

Consequently, we propose the following recommendation.

**Recommendation 1D**

In order to further implement enhanced cooperation, we recommend to invite ICANN to provide to all governments equal treatment with respect to their ccTLDs.

Specifically, it is proposed to invite ICANN to agree to exchange letters with any country that so requests, stating that it will not take any action to re-delegate the country's ccTLD without first obtaining express written approval from the government of the country in question.

And it is proposed to invite ICANN to delegate to any country that so requests up to three additional ccTLDs, with names of the form "ccXYZ", where "cc" is the two-letter country code, and "XYZ" are strings chosen by the country, for example "gov", "mil", "edu", or "01", "02", "03". Thus, if "rt" were a valid country code (which it is not), the corresponding country could request delegation of "rtgov" or "rt01" etc.

**11.2 Agreements regarding jurisdiction**

In the process of revising its bylaws as part of the IANA transition process, the Internet Corporation for Assigned Names and Numbers (ICANN) has explicitly chosen to subject itself to the laws of California, see for example articles 6.1(a) and 24.1 of the new bylaws[183]. Further, ICANN's articles of incorporation[184] specify that it is a California corporation. Article 6 of the bylaws and the articles of incorporation can only by changed upon approval by a three-fourths vote of all the Directors and the approval of the Empowered Community[185]. A change to a fundamental bylaw is approved by the Empowered Community only if it is not objected to by more than one member of that body[186].

Since ICANN is legally a US entity, it is subject to the jurisdiction of US courts[187]. US courts have exercised that jurisdiction in the past[188].

---

[183] https://www.icann.org/en/system/files/files/adopted-bylaws-27may16-en.pdf
[184] https://www.icann.org/resources/pages/governance/articles-en
[185] See article 25 and 25.2(b).
[186] See 1.4(b)(ii) of the Annex D of the bylaws.
[187] A detailed explanation of why this is significant, including the historical background of the issue, is provided at: http://cis-india.org/internet-governance/blog/jurisdiction-the-taboo-topic-at-icann ; a shorter account is provided at:
http://www.epw.in/journal/2016/42/web-exclusives/internet-governance.html ; see also:
http://www.internetgovernance.org/2017/07/20/icann-and-jurisdiction-working-group-reaches-critical-juncture/
[188] See for example https://www.icann.org/news/announcement-2-2016-03-05-en and
https://www.prlog.org/12539064-united-states-court-has-granted-an-interim-relief-for-dca-trust-on-africa.html
and the court case filed just prior to the IANA transition:
https://www.texasattorneygeneral.gov/files/epress/Net_Complaint_-_FILED.pdf
http://ia601506.us.archive.org/17/items/gov.uscourts.txsd.1386946/gov.uscourts.txsd.1386946.7.0.pdf

In line with the principles of equal footing and equal roles and responsibilities of all governments enunciated in the Tunis Agenda, ICANN should not be subject to the jurisdiction of a particular country.

One solution would be for the USA (or some other country) to grant some form of immunity to ICANN.

But, since ICANN has chosen to subject itself to the jurisdiction of the USA, it does not appear that ICANN would accept some form of immunity. Therefore it seems more appropriate to recommend what follows in order to avoid a court ordering ICANN to re-delegate a ccTLD or to reassign IP addresses[189].

**Recommendation 13**

We recommend to invite concerned states to make a binding agreement with each other to the effect that they would not exercise their jurisdiction over ICANN in ways that would violate the principles of equal footing and equal roles and responsibilities of all governments.

Such a binding agreement would have to take the form of a treaty. The exact language of the treaty would have to be carefully negotiated. Therefore we also propose the following.

**Recommendation 14**

We recommend to invite concerned states to consider the matter of agreeing to refrain to exercise jurisdiction over ICANN in certain ways and to convene a treaty negotiation on this matter.

Further, the IANA transition process provides that the management and operation of the authoritative root zone server will continue to be provided by Verisign, but under a contract with ICANN, and not under a contract with the US government as was the case in the past.[190]

This decision was not the result of a public consultation. Verisign is a US company, subject to US jurisdiction, so US courts could order Verisign directly to change the root, they don't necessarily need to order ICANN to do so. So long as Verisign had a contract with the US government, it was unlikely that Verisign could be sued directly, because it was just implementing whatever NTIA told it do. But now the US government is no longer in the loop, so Verisign can be sued directly.

Further, ten of the thirteen root servers which provide the data used by all other instances of root servers are managed by US entities (three of which are US government agencies: NASA, Defense Systems Information Agency, and US Army); the other three servers are managed by entities in Japan,

---

http://ia601506.us.archive.org/17/items/gov.uscourts.txsd.1386946/gov.uscourts.txsd.1386946.10.1.pdf

A full compendium of litigation concerning ICANN is found at:
https://www.icann.org/resources/pages/governance/litigation-en

[189] This example is not theoretical. The equivalent of such remedies, namely "attachment" has been requested in a lawsuit involving Iran, see: https://www.icann.org/resources/pages/icann-various-2014-07-30-en
and in particular page 1 of https://www.icann.org/en/system/files/files/appellants-brief-26aug15-en.pdf .

[190] https://www.icann.org/news/blog/root-zone-management-transition-update-preservation-of-security-stability-and-resiliency

the Netherlands, and Sweden.[191] An operator of a root server could misuse it in various ways, in particular to collect certain types of data or to degrade certain services.[192]

We propose the following recommendation to address these matters.

**Recommendation 15**

We recommend to invite all concerned states to enter into a binding agreement to the effect that they will not exercise their jurisdiction over any root zone server, or over the operator of the authoritative root zone file, in ways that would violate the principles of equal footing and equal roles and responsibilities of all governments.

**Recommendation 16** is included in the above and is hereby withdrawn.

**11.3 Protection of country names in the DNS**

In 2000, the World Intellectual Property Organization was requested by 20 states to study certain intellectual property issues relating to Internet domain names that had not been considered in the First WIPO Internet Domain Name Process, including protection of geographic identifiers.[193]

WIPO duly studied the issues and, on 21 February 2003, informed ICANN[194] that its Member States formally recommended, inter alia, that country names should be protected against abusive registration as domain names. The decision to make that recommendation was supported by all Member States of WIPO, with the exception of Australia, Canada and the United States of America, which dissociated themselves from the decision. Japan also expressed certain reservations. WIPO recommended that the protection of country names should be implemented through an amendment of the Uniform Dispute Resolution Policy (UDRP) and should apply to all future registrations of domain names in the gTLDs.

The recommendation was discussed in ICANN, but it was not agreed and, consequently, the UDRP was not modified. Thus, at present, the UDRP does not protect country names.

Following the privatization of ICANN on 1 November 2016, this matter was brought to the attention of the ITU World Telecommunication Standardization Assembly (WTSA) in Addendum 22 to Document 42-E[195], which states:

> There are two main categories of Top Level Domains, Country Code (ccTLDs) and Generic (gTLDs). One of the differences between the administration of the ccTLDs and the gTLDs is the national sovereignty of the administration of the ccTLDs as opposed to the global and ICANN managed administration of gTLDs.
>
> While WTSA focuses on ccTLDs, the recent expansion of generic TLDs initiated in 2012 by ICANN introduced many new applications some that have geographic implications, which require

[191] See https://en.wikipedia.org/wiki/Root_name_server
[192] See http://www.cavebear.com/old_cbblog/000232.html
[193] http://www.wipo.int/amc/en/processes/process2/index.html
[194] http://www.wipo.int/export/sites/www/amc/en/docs/wipo.doc
[195] http://www.itu.int/md/T13-WTSA.16-C-0042/en

addressing various challenges, including resolution of various conflicts. **Therefore "*special attention should be given to the issue of geographic gTLDs as a concept (in generic terms), as they intersect with core areas of interests of any state*"**.

The submission to WTSA provides a summary of events relating to the delegation of the gTLD ".africa" and states:

> These challenges to delegating a regional geographic Top Level Domain raises important principle concerns for the Africa region and others over the issue of jurisdiction, who should control the delegation of critical regional geographic names like dot Africa, the role of governments and intergovernmental organizations in the ICANN multi-stakeholder model and the effectiveness and reliability of government protection mechanisms for ccTLDs and geographic names related to their distinct regions.

The submission to WTSA proposed, inter alia, to instruct ITU-T Study Group 2:

> 2 to study necessary measures that should be taken to ensure that country, territory and regional names must be protected and reserved from registration as new gTLDs; and that these names should include but not be limited to capital cities, cities, sub-national place names (county, province or state) and geographical indications;
>
> 3 to study, in collaboration with relevant bodies, on ways and means to maintain the right of Member States to request the reservation and to oppose the delegation of any top-level domain (even if it is not included on that list) on the basis of its sensitivity to regional and national interests,

The matter was discussed at WTSA, but no agreement was reached on whether ITU-T should study the matter, and if so how[196]. Consequently, the following recommendation is proposed.

**Recommendation 17**

We recommend to invite all concerned countries to transpose into their national law the WIPO recommendations of 21 February 2003 regarding the protection of country names against abusive registration as domain names, so that they could be enforced in all countries that have jurisdiction over ICANN.

### 11.4 OFAC licenses

**Recommendation 19D**

We recommend to facilitate participation by individuals and/or entities from certain countries in ICANN matters[197] by inviting ICANN to consider taking the following actions:

[196] See DT/60, http://www.itu.int/md/T13-WTSA.16-161025-TD-GEN-0060/en

[197] For the background, see: http://www.internetgovernance.org/2017/01/13/icanns-jurisdiction-sanctions-and-domain-names/ and http://www.internetgovernance.org/2017/07/20/icann-and-jurisdiction-working-group-reaches-critical-juncture/

1. Request a general OFAC waiver from the U.S. Commerce Department

2. Contractually oblige registrars to investigate the possibility of receiving an OFAC license for providing services to sanctioned countries

3. Prohibit registrars from arbitrarily cancelling domain names without notice

4. Obtain a legal opinion regarding whether registrars based in other countries need to comply with OFAC and US laws in general

5. Take any other actions which may alleviate the problem

**12. Roles and Responsibilities**

**Recommendation 18**

We recommend to invite all stakeholders to consider revisiting the roles and responsibilities of the several stakeholders outlined in paragraph 35 of the Tunis Agenda in light of developments and discussions that have taken place over the past 10 years. Specifically, we recommend considering the following revisions to paragraph 35 of the Tunis agenda:

**35. We reaffirm** that the management of the Internet encompasses both technical and public policy issues, which may be inter-related, and should involve all stakeholders and relevant intergovernmental and international organizations. Decisions should always be informed as appropriate by inputs from stakeholders. In this respect it is recognized that:

**a)** Policy authority for Internet-related public policy issues is the sovereign right of States. They have rights and responsibilities for ~~international~~ Internet-related public policy issues, and in particular for the protection of all human rights. Decisions should be informed by inputs from other stakeholders as appropriate.

**b)** The private sector has had, and should continue to have, an important role in the development of the Internet, both in the technical and economic fields, and in providing objective factual information to policy decision-makers, so as to further the public interest and to achieve the shared goal of an equitable information society.

**c)** Civil society has also played an important role on Internet matters, ~~especially at community level~~ at both the national and international levels, and should continue to play such a role. Further, it should provide views, opinions, and information to policy decision-makers and should be invited to comment, as appropriate, regarding public policy issues at both the national and international levels. Representatives, if representation is needed, should be selected through open, democratic, and transparent processes. Internal processes should be based on inclusive, publicly known, well defined and accountable mechanisms.

**d)** Intergovernmental organizations have had, and should continue to have, a facilitating role in the coordination of Internet-related public policy issues and in the harmonization of national laws and practices.

**e)** International organizations have also had and should continue to have an important role in the development of Internet-related technical standards and relevant policies.

The respective roles and responsibilities of stakeholders should be interpreted in a flexible manner with reference to the issue under discussion.