

## **Contribution to the October 2017-January 2018 Open Consultation of the ITU CWG-Internet**

28 September 2017

Richard Hill<sup>1</sup>, APiG

### **Summary**

The factors impede Internet access and digital literacy of women and girls are largely the factors that we have discussed in our previous submissions to CWG-Internet, in particular the urgent need to reduce the cost of connectivity in developing countries. This can be achieved by fostering competition (which may include functional separation), funding infrastructure, taking steps to reduce the cost of international connectivity, supporting the development of local content, capacity building, and a proper governance system.

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

The body of the paper contains specific recommendations for each of these issues, as well as specific recommendations regarding how to address the under-representation of women in key decision-making structures in the ITU.

### **Background and Introduction**

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

CWG-Internet invites all stakeholders to submit contributions on achieving gender equality for Internet users, focusing on the following questions:

1. What approaches and examples of good practices are available to increase Internet access and digital literacy of women and girls, including in decision-making processes on Internet public policy?
2. What approaches and examples of good practices are available to promote the access and use of ICTs by SMEs in developing and least-developed countries, particularly those owned/managed by women, in order to achieve greater participation in the digital economy?
3. Which are the available sources and mechanisms for measuring women's participation in the digital economy with focus on SME's and micro-enterprises?
4. What measures/policies could be envisioned in order to foster the role of women as entrepreneurs and managers of SMEs, specifically in developing and least-developed countries?
5. What are the gaps in addressing these challenges? How can they be addressed and what is the role of governments?"

---

<sup>1</sup> [info@apig.ch](mailto:info@apig.ch)

## **1. Approaches and examples of good practices to increase Internet access and digital literacy of women and girls**

In order to address this question, it is first important to understand what factors impede Internet access and digital literacy of women and girls.

Many of those factors are well presented in the 5 May 2017 Report of the United Nations High Commissioner for Human Rights UN-HCHR), document A/HRC/35/9, "Promotion, protection and enjoyment of human rights on the Internet: ways to bridge the gender digital divide from a human rights perspective"<sup>2</sup>. Some of those factors are also presented in the March 2017 Report of the Working Group on the Digital Gender Divide of the Broadband Commission "Recommendations for action: bridging the gender gap in Internet and broadband access and use"<sup>3</sup>.

We cite from the UN-HCHR report:

11. Factors influencing, preventing or inhibiting women's access and use of ICTs may include:
  - (a) Availability: for example, the status and degree of infrastructural roll-out, barriers to broadband access and limitations on women accessing public Internet places;
  - (b) Affordability: with more limited financial resources, women are disproportionately affected;
  - (c) Sociocultural barriers: for example, time, mobility and gender roles, norms and stereotypes;
  - (d) Legislation, policies or practices: for example, regulation of the licensing of ICTs, subscription services, discriminatory policies and practices that affect women;
  - (e) Education, capacity and skills development: for example, illiteracy and a lack of digital skills and confidence;
  - (f) Privacy, security, trust and safety risks: for example, online harassment and violence against women;
  - (g) Relevant content, applications and services: for example, a lack of content that speaks to women's diverse realities or that has perceived benefit, or censorship or restriction of gender-related content;
  - (h) ICT development, policy and governance: for example, the absence of women in technology-related careers, in ICT leadership positions and in key Internet governance decision-making structures

...

---

<sup>2</sup> [http://ap.ohchr.org/documents/dpage\\_e.aspx?si=A/HRC/35/9](http://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/35/9)

<sup>3</sup> See in particular page 9 at <http://broadbandcommission.org/Documents/publications/WorkingGroupDigitalGenderDivide-report2017.pdf>

18. The General Assembly, the United Nations High Commissioner for Human Rights and several special rapporteurs have recognized that privacy is a prerequisite for the full exercise of other rights, notably the right to freedom of opinion and expression. Women's right to privacy in the context of equal access to ICTs implies the ability to benefit from encryption, anonymity or the use of pseudonyms on social media in order to minimize the risk of interference with privacy, which is especially pertinent for women human rights defenders and women trying to obtain information otherwise considered taboo in their societies.

19. At the same time, the use of ICTs could result in arbitrary or unlawful interference in women's privacy, for example through surveillance and monitoring of women's correspondence and activities, or in targeted attacks on women's privacy through the publication of personal data and information on the Internet ("doxing"). Big data also poses particular challenges to women's right to privacy, for example during the collection, storage, sharing and repurposing of large sets of data, which may involve the potential for re-identification, de-anonymization and aggregation of information. Of particular concern is the potential danger posed to the privacy of marginalized women when big data is used for development or humanitarian purposes. While big data may carry benefits for development initiatives, it also carries serious risks, which are often ignored.

20. The Internet is a key means by which individuals can exercise the right to freedom of opinion and expression. This right includes the freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers and through any media.

...

41. Another widely shared concern is that of algorithmic discrimination and bias. Studies indicate that as the use of artificial intelligence systems becomes more pervasive, there may be disproportionate and disparate impacts on certain groups facing systemic inequalities, including women within those groups

...

47. States and business enterprises should adopt proactive measures to ensure women's equal and meaningful participation online, including by addressing the underrepresentation of women in science, technology and engineering sectors, particularly in leadership positions.

Similar issues and factors were identified in 2016 by the Association for Progressive Computing in its Feminist Principles of the Internet - Version 2.0<sup>4</sup> (which also identified other issues).

We comment on the factors listed above and offer recommendations to ameliorate the situation.

---

<sup>4</sup> <http://www.apc.org/en/pubs/feminist-principles-internet-version-20>

## **1.1 Availability and affordable access**

The importance of affordable access, in particular for women in developing countries, was well highlighted in the 11 May 2017 summary of a roundtable discussion convened by the Internet Society and Chatham House<sup>5</sup>: “The Internet is for everyone, according to the Internet Society’s vision, but it has not quite happened for all. Access to the Internet is essential for empowerment of certain groups, especially women, connecting them with global markets and communities. Yet, women in Africa are 50 per cent less likely to be online than men; and there are digital divides also affecting people with disabilities, and people lacking digital skills.” The same point is made, and well documented by data, in the 25 July 2017 Issue Paper “Gender” of the Internet Society Asia-Pacific Bureau.<sup>6</sup>

Users must have affordable access to the Internet. Therefore, it is important to stress once again, that reducing the cost of connectivity must be a priority. We say “once again” because we have already made this point, and provided specific recommendations, in previous submissions to CWG-Internet.<sup>7</sup>

Further, it is important to address the revenue flows of OTT and to ensure that infrastructure providers are adequately compensated. We note that the mandate of Question 9<sup>8</sup> of ITU-T Study Group 3 includes studying the economic impact of OTT and we hope that such studies will address the issues outlined above.

## **1.2 Socio-cultural barriers and the under-representation of women in key decision-making structures**

As the 25 July 2017 Issue Paper “Gender” of the Internet Society Asia-Pacific Bureau aptly puts the matter:<sup>9</sup>

To bridge the gender digital divide, it is necessary to understand the root causes of gender inequality and discrimination, and address the underlying barriers to these inequalities, including gender divides in education, the labour market, political participation, the ownership of resources and decision-making, caused by existing socio-cultural norms, values and attitudes.

We propose that ITU conduct a survey on perceptions of gender diversity in ITU analogous to the one conducted by ICANN in June 2017, see:

<https://www.icann.org/news/announcement-2017-06-12-en>

---

<sup>5</sup> A Brave New World: How Internet Affects Societies, available at:  
<https://www.internetsociety.org/doc/chathamhouse>

<sup>6</sup> <https://www.internetsociety.org/doc/issue-paper-asia-pacific-bureau-%E2%80%93-gender>

<sup>7</sup> See 1.1 of <http://www.itu.int/en/Lists/consultationOct2016/Attachments/24//CWG-Internet%202017.pdf> and 1.2 of <http://www.itu.int/en/Lists/consultationJune2017/Attachments/4//CWG-Internet%202017-2.pdf>

<sup>8</sup> <https://www.itu.int/en/ITU-T/studygroups/2017-2020/03/Pages/q9.aspx>

<sup>9</sup> <https://www.internetsociety.org/doc/issue-paper-asia-pacific-bureau-%E2%80%93-gender>

Further, we propose that the following rules be adopted by the ITU, so as to give an example that can be followed by others:

- Unless otherwise decided by the competent body, all formal meetings and groups shall be co-chaired by two people of different genders; one of the persons shall come from a developing country.
- Delegations to formal meeting shall be headed by two people of different genders.
- In formal meetings, speakers of opposite genders shall alternate: that is, after a woman has taken the floor, a man must be given the floor (and vice versa).
- At least two of the five elected officials must be of a different gender than the other three. The electoral process shall be modified in order to ensure that this is the case.

### **1.3 Education, capacity building, and lack of relevant content**

The development of content (including by women) of content that is relevant for women will be fostered by increasing the education and digital skills of women. It is axiomatic that education requires access to knowledge, including scientific publications. At present, much of that knowledge is protected by copyright.

As noted in paragraphs 1.12 and 1.13 of our submission<sup>10</sup> to a previous consultation, the current dysfunctional copyright and patent regimes result in excessively high costs for access to knowledge, including excessively high costs for hardware and software. Various reports<sup>11</sup> have recently highlighted that point in the context of human rights and development. As recent study put the matter<sup>12</sup>:

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

Intellectual property laws must be reformed to facilitate access by disadvantaged groups, including women, and in particular women in developing countries.

---

<sup>10</sup> <http://www.itu.int/en/council/cwg-internet/Pages/display-feb2016.aspx?ListItemID=13>

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

<sup>12</sup> [http://www.ictsd.org/sites/default/files/research/ceipi-ictsd\\_3\\_0.pdf](http://www.ictsd.org/sites/default/files/research/ceipi-ictsd_3_0.pdf). The citation is from page 14. See also pp. 84 ff. We cite from p. 85: "Copyright, originally conceived as a tool to protect the author and to provide incentives for him or her to create for the benefit of society, is nowadays more and more perceived as an instrument to the advantage of 'large, impersonal and unlovable corporations'. ... Copyright is increasingly perceived as a right to sanction and punish that prevents the free flow of information and access to knowledge or cultural participation, not as a right that has positive effects for the development of society."

#### 1.4 Privacy, encryption, and mass surveillance

We reiterate and amplify comments made in our previous submissions to CWG-Internet.<sup>13</sup>

Privacy is a fundamental right, and any violation of privacy must be limited to what is strictly necessary and proportionate in a democratic society.<sup>14</sup> Certain states practice mass surveillance that violates the right to privacy<sup>15</sup> (see for example A/HRC/31/64<sup>16</sup>, A/71/373<sup>17</sup>, A/HRC/34/60<sup>18</sup> and European Court of Justice judgment<sup>19</sup> 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.<sup>20</sup> As UNCTAD puts the matter<sup>21</sup>:

countries need to implement measures that place appropriate limits and conditions on surveillance. Key measures that have emerged include:

- providing a right to legal redress for citizens from any country whose data is transferred into the country (and subject to surveillance);
- personal data collection during surveillance should be 'necessary and proportionate' to the purpose of the surveillance; and
- surveillance activities should be subject to strong oversight and governance.

At its 34th session, 27 February-24 March 2017, the Human Rights Council (HRC) adopted a new resolution on the Right to privacy in the digital age<sup>22</sup>. That resolution recalls that States should ensure that any interference with the right to privacy is consistent with the principles of legality, necessity and

---

<sup>13</sup> See 2.6 of <http://www.itu.int/en/Lists/consultationJune2017/Attachments/4//CWG-Internet%202017-2.pdf>

<sup>14</sup> 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://supremecourtindia.nic.in/pdf/LU/ALL%20WP\(C\)%20No.494%20of%202012%20Right%20to%20Privacy.pdf](http://supremecourtindia.nic.in/pdf/LU/ALL%20WP(C)%20No.494%20of%202012%20Right%20to%20Privacy.pdf)

<sup>15</sup> 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>

<sup>16</sup> <http://ohchr.org/Documents/Issues/Privacy/A-HRC-31-64.doc>

<sup>17</sup> [http://www.un.org/ga/search/view\\_doc.asp?symbol=A/71/373](http://www.un.org/ga/search/view_doc.asp?symbol=A/71/373)

<sup>18</sup> [http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session34/Documents/A\\_HRC\\_34\\_60\\_EN.docx](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**.

<sup>19</sup> <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>

<sup>20</sup> 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](http://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/35/22)

<sup>21</sup> *Data protection regulations and international data flows: Implications for trade and development*, p. 66, available at: [http://unctad.org/en/PublicationsLibrary/dtlstict2016d1\\_en.pdf](http://unctad.org/en/PublicationsLibrary/dtlstict2016d1_en.pdf)

<sup>22</sup> [http://www.un.org/ga/search/view\\_doc.asp?symbol=A/HRC/34/L.7/Rev.1](http://www.un.org/ga/search/view_doc.asp?symbol=A/HRC/34/L.7/Rev.1)

proportionality.<sup>23</sup> Even a well-known business publication has recognized that privacy is a pressing issue<sup>24</sup>. And many of the issues mentioned in this contribution have been well presented in the 27 July 2017 Issue Paper “Online Privacy” of the Internet Society Asia-Pacific Bureau.<sup>25</sup>

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.”<sup>26</sup>

It appears to us that this decision and questions<sup>27</sup> 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”<sup>28</sup>). 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<sup>29</sup>, 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<sup>30</sup>). Many commentators oppose state-attempts to compromise encryption.<sup>31</sup> The 2016 UNESCO Report “Human rights and encryption” also

---

<sup>23</sup> See 2 of the cited HRC Resolution

<sup>24</sup> <http://www.economist.com/news/briefing/21721634-how-it-shaping-up-data-giving-rise-new-economy>

<sup>25</sup> <https://www.internetsociety.org/doc/issue-paper-asia-pacific-bureau-%E2%80%93-online-privacy>

<sup>26</sup><sup>26</sup> <https://www.whitehouse.gov/the-press-office/2017/01/25/presidential-executive-order-enhancing-public-safety-interior-united>

<sup>27</sup> See for example: <http://www.sophieintveld.eu/letter-to-eu-commission-what-impact-has-trump-decisions-on-privacy-shield-and-umbrella-agreement/>

<sup>28</sup> [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](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)

<sup>29</sup> See for example <https://www.bloomberg.com/news/articles/2017-07-10/australia-s-turnbull-urges-internet-providers-to-block-extremism>

<sup>30</sup> <https://documents-dds-ny.un.org/doc/UNDOC/GEN/G15/095/85/PDF/G1509585.pdf?OpenElement>

<sup>31</sup> See for example pp. vii, 106, and 113 of GCI. 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>

points out that attempts to limit the use of encryption, or to weaken encryption methods, may impinge on freedom of expression and the right to privacy.<sup>32</sup> The cited HRC resolution calls on states not to interfere with the use of encryption.<sup>33</sup> The Internet Society recommends the following<sup>34</sup>: “Encryption is and should remain an integral part of the design of Internet technologies, applications and services. It should not be seen as a threat to security. We must strengthen encryption, not weaken it.” And this because “If governments persist in trying to prevent the use of encryption, they put at risk not only freedom of expression, privacy, and user trust, but the future Internet economy as well.”<sup>35</sup>

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.<sup>36</sup>

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<sup>37</sup>. In particular, restrictions must be placed on the collection and aggregation of meta-data.<sup>38</sup>

There does not appear to be adequate consideration of the issues outlined above at the international level.<sup>39</sup>

We recommend to invite IETF, ISOC, ITU, and OHCHR<sup>40</sup> to study the issues of privacy, encryption and prevention of inappropriate mass surveillance, which include technical, user education, and legal aspects.

---

<sup>32</sup> See in particular pp. 54 ff. The Report is at: <http://unesdoc.unesco.org/images/0024/002465/246527e.pdf>

<sup>33</sup> See 9 of the cited HRC Resolution

<sup>34</sup> Page 106 of the 2017 Global Internet Report: Paths to Our Digital Future, available at: <https://future.internetsociety.org/wp-content/uploads/2017/09/2017-Internet-Society-Global-Internet-Report-Paths-to-Our-Digital-Future.pdf>

<sup>35</sup> Page 39 of the cited ISOC report.

<sup>36</sup> See for example p. 66 of GCIIG.

<sup>37</sup> For a specific proposal, see the last page of the proposals at: [https://justnetcoalition.org/sites/default/files/HCHR\\_report\\_final.pdf](https://justnetcoalition.org/sites/default/files/HCHR_report_final.pdf)

<sup>38</sup> See p. 31 of GCIIG.

<sup>39</sup> See paragraph 46 of [http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session34/Documents/A\\_HRC\\_34\\_60\\_EN.docx](http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session34/Documents/A_HRC_34_60_EN.docx)

<sup>40</sup> 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>

## 1.5 Security

We reiterate and amplify comments made in our previous submissions to CWG-Internet.<sup>41</sup>

As the 25 July 2017 Issue Paper “Gender” of the Internet Society Asia-Pacific Bureau puts the matter: “Security and harassment emerged [from a survey] as one of the top five barriers to mobile phone ownership and usage, and is a key concern for women.”<sup>42</sup>

Security experts have long recognized that lack of ICT security creates a negative externality.<sup>43</sup> 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.<sup>44</sup> 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.<sup>45</sup> 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<sup>46</sup>:

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<sup>47</sup> that affected a large number of users and many hospitals.

---

<sup>41</sup> See 2.8 of <http://www.itu.int/en/Lists/consultationJune2017/Attachments/4//CWG-Internet%202017-2.pdf>

<sup>42</sup> <https://www.internetsociety.org/doc/issue-paper-asia-pacific-bureau-%E2%80%93-gender>

<sup>43</sup> [https://www.schneier.com/blog/archives/2007/01/information\\_sec\\_1.html](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/>

<sup>44</sup> See also pp. vii and 66 of GCIG.

<sup>45</sup> [https://en.wikipedia.org/wiki/WannaCry\\_cyber\\_attack](https://en.wikipedia.org/wiki/WannaCry_cyber_attack)

<sup>46</sup> See p. 18 of the cited Global Internet Report 2016.

<sup>47</sup> [https://en.wikipedia.org/wiki/WannaCry\\_cyber\\_attack](https://en.wikipedia.org/wiki/WannaCry_cyber_attack)

As the European Union Agency for Network and Information Security (ENISA) puts the matter<sup>48</sup>: “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)<sup>49</sup>. As a well known security expert puts the matter<sup>50</sup>: “Security engineers are working on technologies that can mitigate much of this risk, but many solutions won't be deployed without government involvement. This is not something that the market can solve. ... the interests of the companies often don't match the interests of the people. ... Governments need to play a larger role: setting standards, policing compliance, and implementing solutions across companies and networks.”

Recent research shows that a perceived lack of security is reducing consumer propensity to use the Internet for certain activities.<sup>51</sup>

Some national authorities are taking some measures.<sup>52</sup> In particular, the President of the USA issued an Executive Order<sup>53</sup> 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<sup>54</sup> 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

---

<sup>48</sup> Preamble of <https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/infineon-nxp-st-enisa-position-on-cybersecurity>

<sup>49</sup> See p. 107 of the cited Global Internet Report 2016.

<sup>50</sup> [https://www.schneier.com/blog/archives/2016/07/real-world\\_secu.html](https://www.schneier.com/blog/archives/2016/07/real-world_secu.html)

<sup>51</sup> <https://www.cigionline.org/internet-survey>

<sup>52</sup> For example, for cybersecurity for motor vehicles, see:

[http://www.nhtsa.gov/About-NHTSA/Press-Releases/nhtsa\\_cybersecurity\\_best\\_practices\\_10242016](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](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)

<sup>53</sup> 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>

**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.<sup>55</sup>

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.

## 1.6 Data and platforms

### 1.6.1 Big data

We reiterate and amplify comments made in our previous submissions to CWG-Internet.<sup>56</sup>

It is obvious that personal data has great value when it is collected on a mass scale and cross-referenced.<sup>57</sup> Indeed, the monetization of personal data drives today’s Internet services and the provision of so-called free services such as search engines.<sup>58</sup> These developments have significant implications, in particular for developing countries.<sup>59</sup> Users should have greater control over the ways in

---

<sup>54</sup> 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>

<sup>55</sup> <http://www.rawstory.com/2017/06/germanys-merkel-says-digital-world-needs-global-rules/>

<sup>56</sup> See 2.3 of <http://www.itu.int/en/Lists/consultationJune2017/Attachments/4//CWG-Internet%202017-2.pdf>

<sup>57</sup> 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](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](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.internet-society.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>

<sup>58</sup> <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.internet-society.org/blog/public-policy/2017/03/my-data-your-business>

<sup>59</sup> <http://twm.my/title2/resurgence/2017/319-320/cover03.htm>

which their data are used.<sup>60</sup> 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.<sup>61</sup> 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<sup>62</sup>. The Internet Society recommends the following<sup>63</sup>: “All users should be able to control how their data is accessed, collected, used, shared and stored. They should also be able to move their data between services seamlessly.”

As the Supreme Court of India put the matter in a recent judgment finding that privacy is a fundamental right: “To put it mildly, privacy concerns are seriously an issue in the age of information.”<sup>64</sup>

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”<sup>65</sup> 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<sup>66</sup>.

---

<sup>60</sup> See for example pp. 42, 106 and 113 of GCI. 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](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](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](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>

<sup>61</sup> <https://www.theguardian.com/technology/2017/jun/04/surge-pricing-comes-to-the-supermarket-dynamic-personal-data>

<sup>62</sup> <https://gizmodo.com/before-you-hit-submit-this-company-has-already-logge-1795906081?null>

<sup>63</sup> Page 107 of the 2017 Global Internet Report: Paths to Our Digital Future, available at : <https://future.internetsociety.org/wp-content/uploads/2017/09/2017-Internet-Society-Global-Internet-Report-Paths-to-Our-Digital-Future.pdf>

<sup>64</sup> 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://supremecourtfindia.nic.in/pdf/LU/ALL%20WP\(C\)%20No.494%20of%202012%20Right%20to%20Privacy.pdf](http://supremecourtfindia.nic.in/pdf/LU/ALL%20WP(C)%20No.494%20of%202012%20Right%20to%20Privacy.pdf)

<sup>65</sup> <http://www.pnas.org/content/110/15/5802.full#aff-1>

<sup>66</sup> <https://www.theguardian.com/commentisfree/2017/jun/18/google-not-gchq--truly-chilling-spy-network> and <https://www.socialcooling.com/>

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.<sup>67</sup>

All states should have comprehensive data protection legislation.<sup>68</sup> The development of so-called “smart cities” might result in further erosion of individual control of personal data. As one journalist puts the matter<sup>69</sup>: “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<sup>70</sup>.

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”<sup>71</sup> companies.

Further, mass-collected data (so-called “big data”<sup>72</sup>) are increasingly being used, via computer algorithms, to make decisions that affect people’s lives, such as credit rating, availability of insurance, etc.<sup>73</sup> 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.

---

<sup>67</sup> 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>

<sup>68</sup> See for example p. 42 of GCIG; and section 5 of <http://www.itu.int/en/council/cwg-internet/Pages/display-feb2016.aspx?ListItemID=70>. A summary of adoption of data protection and data privacy laws by country can be found at: [http://unctad.org/en/Pages/DTL/STI\\_and ICTs/ICT4D-Legislation/eCom-Data-Protection-Laws.aspx](http://unctad.org/en/Pages/DTL/STI_and ICTs/ICT4D-Legislation/eCom-Data-Protection-Laws.aspx)

<sup>69</sup> <https://www.theguardian.com/cities/2014/dec/22/the-smartest-cities-rely-on-citizen-cunning-and-unglamorous-technology>

<sup>70</sup> See “Stop rampant workplace surveillance” on p. 12 of: <http://library.fes.de/pdf-files/id-moe/12797-20160930.pdf>

<sup>71</sup> <http://thelongandshort.org/society/war-on-cash>

<sup>72</sup> 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](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>

<sup>73</sup> <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>

An excellent analysis of the human rights dimensions of algorithms is found in Council of Europe document MSI-NET(2016)06<sup>74</sup>, which makes a number of recommendations for government actions.

It is important to avoid that “big data”, and the algorithmic treatment of personal data, do not result in increased inequality<sup>75</sup> and increased social injustice<sup>76</sup> which would threaten democracy.<sup>77</sup> A balanced discussion of the issues in the context of urban centers is given in a well-researched 2017 white paper by CITRIS Connected Communities Initiative.<sup>78</sup> See also the discussion on pp. 75 ff. of the 2017 Internet Society Global Internet Report: Paths to Our Digital Future<sup>79</sup>.

As learned scholars have put the matter<sup>80</sup>:

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

---

<sup>74</sup> <https://rm.coe.int/16806a7ccc>

<sup>75</sup> <https://inequality.org/facts/income-inequality/>

<sup>76</sup> 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](https://bigdatawg.nist.gov/pdf/big_data_privacy_report_may_1_2014.pdf)

<sup>77</sup> 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/>

<sup>78</sup> [http://citris-uc.org/wp-content/uploads/2017/07/Inclusive-AI\\_CITRIS\\_2017.pdf](http://citris-uc.org/wp-content/uploads/2017/07/Inclusive-AI_CITRIS_2017.pdf)

<sup>79</sup> <https://future.internetsociety.org/wp-content/uploads/2017/09/2017-Internet-Society-Global-Internet-Report-Paths-to-Our-Digital-Future.pdf>

<sup>80</sup> 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>

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."<sup>81</sup>

Control of large amounts of data may lead to dominant positions that impeded competition<sup>82</sup>. 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."<sup>83</sup>

While some national legislators and/or courts have taken steps to strengthen citizens' rights to control the way their personal data are used<sup>84</sup>, to consider product liability issues related to data<sup>85</sup>, and to consider the impact of big data with respect to prohibitions of discrimination in hiring<sup>86</sup>, there does not appear to be adequate consideration of this issue at the international level.<sup>87</sup> Yet failure to address the issue at the international level can have negative consequences, including for trade. As UNCTAD puts the matter<sup>88</sup>:

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.

...

---

<sup>81</sup> <https://www.theguardian.com/world/2017/aug/23/silicon-valley-big-data-extraction-amazon-whole-foods-facebook>

<sup>82</sup> <https://www.wired.com/story/ai-and-enormous-data-could-make-tech-giants-harder-to-topple/>

<sup>83</sup> <https://www.theguardian.com/commentisfree/2016/dec/04/data-populists-must-seize-information-for-benefit-of-all-evgeny-morozov>

<sup>84</sup> 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/>

<sup>85</sup> <http://www.wablegal.com/european-commission-publishes-roadmap-future-proof-eu-product-liability-directive/>

<sup>86</sup> <https://www.eeoc.gov/eeoc/meetings/10-13-16/index.cfm>

<sup>87</sup> Indeed, a group of scholars has called for the creation of a charter of digital rights, see:

<http://www.dw.com/en/controversial-eu-digital-rights-charter-is-food-for-thought/a-36798258>

See also the UNCTAD study at: [http://unctad.org/en/PublicationsLibrary/dtlstict2016d1\\_en.pdf](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>

<sup>88</sup> *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](http://unctad.org/en/PublicationsLibrary/dtlstict2016d1_en.pdf)

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”<sup>89</sup>.

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<sup>90</sup>. 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.<sup>91</sup> We also note that the BRICS Leaders Xiamen Declaration<sup>92</sup> (4 September 2017) stated in its paragraph 13 (emphasis added): “We will advocate the establishment of internationally applicable rules for security of ICT infrastructure, data protection and the Internet that can be widely accepted by all parties concerned, and jointly build a network that is safe and secure.”

Regarding algorithmic use of data, what a UK parliamentary committee<sup>93</sup> said at the national level can be transposed to the international level:

After decades of somewhat slow progress, a succession of advances have recently occurred across the fields of robotics and artificial intelligence (AI), fuelled by the rise in computer processing power, the profusion of data, and the development of techniques such a ‘deep learning’. Though the capabilities of AI systems are currently narrow and specific, they are, 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

---

<sup>89</sup> <https://icdppc.org/wp-content/uploads/2015/02/Montreux-Declaration.pdf>

<sup>90</sup> [http://www.un.org/ga/search/view\\_doc.asp?symbol=A/HRC/34/L.7/Rev.1](http://www.un.org/ga/search/view_doc.asp?symbol=A/HRC/34/L.7/Rev.1)

<sup>91</sup> See 5(f) and 5(k) of the cited Resolution

<sup>92</sup> Available at: [http://www.mea.gov.in/Uploads/PublicationDocs/28912\\_XiamenDeclaratoin.pdf](http://www.mea.gov.in/Uploads/PublicationDocs/28912_XiamenDeclaratoin.pdf)

<sup>93</sup> <http://www.publications.parliament.uk/pa/cm201617/cmselect/cmsctech/145/14502.htm>

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<sup>94</sup> 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.<sup>95</sup>

And experts speaking at a conference<sup>96</sup> on Artificial Intelligence hosted by the ITU raised many of the issues raised in this paper<sup>97</sup>, 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<sup>98</sup>, as did a report by the UK Royal Society<sup>99</sup>, as did the Internet Society in pages 31 ff. of its 2017 Global Internet Report: Paths to Our Digital Future<sup>100</sup>. An academic treatment of the issues is given in Wachter, S., Mittelstadt, B., and Floridi, L. (2017) "Transparent, explainable, and accountable AI for robotics", *Science Robotics*, 31 May 2017, Vol. 2, Issue 6, ean6080, DOI: 10.1126/scirobotics.aan6080<sup>101</sup>.

---

<sup>94</sup> [https://www.nitrd.gov/news/national\\_ai\\_rd\\_strategic\\_plan.aspx](https://www.nitrd.gov/news/national_ai_rd_strategic_plan.aspx)

<sup>95</sup> 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>

<sup>96</sup> <http://www.itu.int/en/ITU-T/AI/Pages/201706-default.aspx>

<sup>97</sup> 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/>

<sup>98</sup> [https://artificialintelligencenow.com/media/documents/AINowSummaryReport\\_3\\_RpmwKHu.pdf](https://artificialintelligencenow.com/media/documents/AINowSummaryReport_3_RpmwKHu.pdf)

<sup>99</sup> <https://royalsociety.org/topics-policy/projects/machine-learning/>

<sup>100</sup> <https://future.internetsociety.org/wp-content/uploads/2017/09/2017-Internet-Society-Global-Internet-Report-Paths-to-Our-Digital-Future.pdf>

<sup>101</sup> <http://robotics.sciencemag.org/content/2/6/ean6080>

We recommend to invite UNCTAD<sup>102</sup> and UNCITRAL to study the issues related to the economic and social value of data, in particular “big data” and the increasing use of algorithms (including artificial intelligence<sup>103</sup>) to make decisions<sup>104</sup>, which issues include economic and legal aspects. In particular, UNCITRAL should be mandated to develop model laws, and possibly treaties, on personal data protection<sup>105</sup>, algorithmic transparency and accountability<sup>106</sup>, and artificial intelligence<sup>107</sup>; UNCTAD

---

<sup>102</sup> 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](http://unctad.org/en/PublicationsLibrary/dtlstict2016d1_en.pdf) ; we also note the newly created Intergovernmental Group of Experts on E-Commerce, see:  
<http://unctad.org/en/Pages/MeetingDetails.aspx?meetingid=1437>

<sup>103</sup> For a discussion of some of the issues related to AI, see:  
[https://www.wired.com/2017/02/ai-threat-isnt-skyline-end-middle-class/?mbid=nl\\_21017\\_p3&CNDID=42693809](https://www.wired.com/2017/02/ai-threat-isnt-skyline-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.internet-society.org/doc/artificial-intelligence-and-machine-learning-policy-paper>

<sup>104</sup> Specific recommendations regarding how to address the issues are found in Section 8, Conclusions and Recommendations, of the September 2016 Council of Europe document “Draft Report on the Human Rights Dimensions of Algorithms” (MSI-NET(2016)06) , available at:  
<https://rm.coe.int/16806a7ccc>

<sup>105</sup> 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](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://supremecourtindia.nic.in/pdf/LU/ALL%20WP\(C\)%20No.494%20of%202012%20Right%20to%20Privacy.pdf](http://supremecourtindia.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> .

Guidelines/best practices could be based on sections 3-9 of the Council of Europe’s T-PD consultative committee’s January 2017 *Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data*, available at: <https://rm.coe.int/16806ebe7a> .

<sup>106</sup> 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](https://www.acm.org/binaries/content/assets/public-policy/2017_usacm_statement_algorithms.pdf)

<sup>107</sup> 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/>

should be mandated to develop a study on the taxation of robots<sup>108</sup>; and the UN Conference on Disarmament should consider taking measures with respect to lethal autonomous weapons<sup>109</sup>.

### 1.6.2 Platform dominance

We reiterate and amplify comments made in our previous submissions to CWG-Internet.<sup>110</sup>

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<sup>111</sup>. If the dominance is due to a better service offer, then market forces are at work and there is no need for regulatory intervention.

But if the dominance is due to economies of scale and network effects<sup>112</sup>, then a situation akin to a natural monopoly<sup>113</sup> might arise, there might be abuse of dominant market power<sup>114</sup>, and regulatory intervention is required<sup>115</sup>. For example, platforms might abusively use personal data to set high prices

---

<sup>108</sup> <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>

<sup>109</sup> A Governmental Group of Experts on this topic has been created, see: [https://www.unog.ch/80256EE600585943/\(httpPages\)/F027DAA4966EB9C7C12580CD0039D7B5?OpenDocument](https://www.unog.ch/80256EE600585943/(httpPages)/F027DAA4966EB9C7C12580CD0039D7B5?OpenDocument)

<sup>110</sup> See 2.11 of <http://www.itu.int/en/Lists/consultationJune2017/Attachments/4//CWG-Internet%202017-2.pdf>

<sup>111</sup> <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/>

<sup>112</sup> 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/>

<sup>113</sup> [https://en.wikipedia.org/wiki/Natural\\_monopoly](https://en.wikipedia.org/wiki/Natural_monopoly)

<sup>114</sup> <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](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](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](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 World Development Report (WDR-2016), titled "Digital Dividends", available at:

<http://documents.worldbank.org/curated/en/896971468194972881/pdf/102725-PUB-Replacement-PUBLIC.pdf>

<sup>115</sup> 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

for goods for certain customers,<sup>116</sup> or a dominant search engine might provide search results that favor certain retail sites<sup>117</sup>, or a dominant national provider might impede the operation of an international competitor<sup>118</sup>, or a dominant company may excessively influence governments<sup>119</sup>. As the Internet Society puts the matter on page 40 of its 2017 Global Internet Report: Paths to Our Future<sup>120</sup>: “ ... the scope of market change driven by dramatic advances in technology will inevitably force a fundamental rethink of existing approaches in competition law and traditional communications regulation. Data will increasingly be seen as an asset linked to competitive advantage, changing the nature of merger reviews, evaluations of dominance and, importantly, consumer protection.”

Further, as already noted, control of large amounts of data may lead to dominant positions that impeded competition<sup>121</sup>. As a learned commentator puts the matter<sup>122</sup>:

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 present competition or anti-trust policies.<sup>123</sup> As one commentator puts the matter<sup>124</sup> (his text starts with a citation):

---

<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.

<sup>116</sup> <https://www.theguardian.com/technology/2017/jun/04/surge-pricing-comes-to-the-supermarket-dynamic-personal-data>

<sup>117</sup> 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_STATEMENT-17-1806_en.htm)  
[http://europa.eu/rapid/press-release\\_MEMO-17-1785\\_en.htm](http://europa.eu/rapid/press-release_MEMO-17-1785_en.htm)

<sup>118</sup> <https://techcrunch.com/2016/11/28/ubers-china-app-is-now-separate-from-its-global-app-and-a-nightmare-for-foreigners/>

<sup>119</sup> [http://www.huffingtonpost.com/entry/google-monopoly-barry-lynn\\_us\\_59a738fde4b010ca289a1155?section=us\\_politics](http://www.huffingtonpost.com/entry/google-monopoly-barry-lynn_us_59a738fde4b010ca289a1155?section=us_politics) and  
<https://www.nakedcapitalism.com/2017/08/new-america-foundation-head-anne-marie-slaughter-botches-launders-googles-money.html>

<sup>120</sup> <https://future.internetsociety.org/wp-content/uploads/2017/09/2017-Internet-Society-Global-Internet-Report-Paths-to-Our-Digital-Future.pdf>

<sup>121</sup> <https://www.wired.com/story/ai-and-enormous-data-could-make-tech-giants-harder-to-topple/>

<sup>122</sup> <https://www.theguardian.com/commentisfree/2016/dec/04/data-populists-must-seize-information-for-benefit-of-all-evgeny-morozov>

<sup>123</sup> <https://www.competitionpolicyinternational.com/let-the-right-one-win-policy-lessons-from-the-new-economics-of-platforms/>  
[https://www.washingtonpost.com/business/is-amazon-getting-too-big/2017/07/28/ff38b9ca-722e-11e7-9eac-d56bd5568db8\\_story.html](https://www.washingtonpost.com/business/is-amazon-getting-too-big/2017/07/28/ff38b9ca-722e-11e7-9eac-d56bd5568db8_story.html) .

*“I do not divide monopolies in private hands into good monopolies and bad monopolies. There is no good monopoly in private hands until the Almighty sends us angels to preside over the monopoly. There may be a despot who is better than another despot, but there is no good despotism’*

William Jennings Bryan, speech, 1899, quoted in Hofstadter (2008)

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

As a scholar puts the matter<sup>125</sup>:

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

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

As noted above, the dominance of certain platforms<sup>126</sup> raises issues related to freedom of speech, because some platforms apply strict rules of their own to censor certain types of content<sup>127</sup>, and, for

---

An academic treatment of the topic is Khan, L. M. (2017) “Amazon’s Antitrust Paradox”, *The Yale Law Journal*, vol. 126, no. 3, pp. 564-907, available at: <http://www.yalelawjournal.org/note/amazons-antitrust-paradox>

<sup>124</sup> 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>

<sup>125</sup> Khan, L. M. (2017) “Amazon’s Antitrust Paradox”, *The Yale Law Journal*, vol. 126, no. 3, pp. 564-907, available at: <http://www.yalelawjournal.org/note/amazons-antitrust-paradox>

many users, there are no real alternatives to dominant platforms<sup>128</sup>; and some workers might also face limited choices due to dominant platforms<sup>129</sup>.

As *The Economist* puts the matter<sup>130</sup>:

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.<sup>131</sup>

And, citing *The Economist* again<sup>132</sup>:

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 ...

---

<sup>126</sup> For data regarding such dominance, see for example:

[http://www.eecs.umich.edu/eecs/about/articles/2009/Observatory\\_Report.html](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/>

<sup>127</sup> See for example [https://www.theguardian.com/technology/2016/sep/09/facebook-deletes-norway-pms-post-  
napalm-girl-post-row](https://www.theguardian.com/technology/2016/sep/09/facebook-deletes-norway-pms-post-napalm-girl-post-row)

<sup>128</sup> [https://www.theguardian.com/technology/2016/nov/17/google-suspends-customer-accounts-for-reselling-  
pixel-phones](https://www.theguardian.com/technology/2016/nov/17/google-suspends-customer-accounts-for-reselling-pixel-phones)

<sup>129</sup> [https://www.nytimes.com/2017/03/21/magazine/platform-companies-are-becoming-more-powerful-but-  
what-exactly-do-they-want.html?\\_r=2](https://www.nytimes.com/2017/03/21/magazine/platform-companies-are-becoming-more-powerful-but-what-exactly-do-they-want.html?_r=2)

<sup>130</sup> [http://www.economist.com/news/leaders/21707210-rise-corporate-colossus-threatens-both-competition-and-  
legitimacy-business](http://www.economist.com/news/leaders/21707210-rise-corporate-colossus-threatens-both-competition-and-legitimacy-business)

<sup>131</sup> <https://disruptive.asia/transit-dead-content-literally-rules/>

<sup>132</sup> <http://www.economist.com/news/briefing/21721634-how-it-shaping-up-data-giving-rise-new-economy>

As learned scholars have put the matter<sup>133</sup>:

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 only with respect to users and consumers.<sup>134</sup>

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.”<sup>135</sup>

National authorities in a number of countries have undertaken investigations,<sup>136</sup> and even imposed measures,<sup>137</sup> 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.”<sup>138</sup> The Legal Affairs Committee of the European Parliament adopted an Opinion in May 2017 that, among other provisions<sup>139</sup>:

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;

---

<sup>133</sup> 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>

<sup>134</sup> [https://www.nytimes.com/interactive/2017/04/02/technology/uber-drivers-psychological-tricks.html?\\_r=2](https://www.nytimes.com/interactive/2017/04/02/technology/uber-drivers-psychological-tricks.html?_r=2)

<sup>135</sup> <https://www.theguardian.com/commentisfree/2016/dec/04/data-populists-must-seize-information-for-benefit-of-all-evgeny-morozov>

<sup>136</sup> See for example [http://europa.eu/rapid/press-release\\_IP-16-1492\\_en.htm](http://europa.eu/rapid/press-release_IP-16-1492_en.htm) ; [http://europa.eu/rapid/press-release\\_IP-16-2532\\_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](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>

<sup>137</sup> See for example [http://www.autoritedelaconurrence.fr/user/standard.php?id\\_rub=606&id\\_article=2534](http://www.autoritedelaconurrence.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](http://europa.eu/rapid/press-release_IP-17-1784_en.htm)

<sup>138</sup> <http://www.cnet.com/news/senator-warren-says-apple-google-and-amazon-have-too-much-power/>

<sup>139</sup> <http://www.europarl.europa.eu/sides/getDoc.do?type=COMPARL&reference=PE-601.100&format=PDF&language=EN&secondRef=02>

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)).<sup>140</sup> And by some provisions in the national laws of at least one country.<sup>141</sup>

However, it does not appear that there is an adequate platform for exchanging national experiences regarding such matters.<sup>142</sup>

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.<sup>143</sup>

We recommend to invite UNCTAD to study the economic and market issues related to platform dominance<sup>144</sup>, and to facilitate the exchange of information on national and regional experiences, and that the ILO be mandated to study the worker protection issues related to platform dominance and the so-called “sharing economy”.

Further, dominant search platforms may, inadvertently or deliberately, influence election results, which may pose an issue for democracy.<sup>145</sup>

---

<sup>140</sup> <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+COMPARG+PE-599.814+01+DOC+PDF+V0//EN&language=EN>

<sup>141</sup> See section 3.2 of the following commentary on the French Digital Republic Law: <https://www.lw.com/thoughtLeadership/French-digital-republic-law-english>

<sup>142</sup> 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>

<sup>143</sup> 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>

<sup>144</sup> We note in this context the existence in UNCTAD of the Intergovernmental Group of Experts on Competition Law and Policy, see: <http://unctad.org/en/Pages/DITC/CompetitionLaw/Intergovernmental-Group-of-Experts-on-Competition-Law-and-Policy.aspx> and the United Nations Set of Rules and Principles on Competition (TD/RBP/CONF/10/Rev.2), published in 2000 and available at: <http://unctad.org/en/docs/tdrbpconf10r2.en.pdf>

<sup>145</sup> <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>

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.

### 1.7 Freedom of expression

We reiterate and amplify comments made in our previous submissions to CWG-Internet.<sup>146</sup>

An increasing number of states have implemented, or are proposing to implement, measures to restrict access to certain types of Internet content<sup>147</sup>, e.g. incitement to violence, gambling, copyright violation, or to take measures<sup>148</sup> 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<sup>149</sup>, 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.<sup>150</sup>

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.<sup>151</sup>

---

for a possible impact on free speech, see:

<http://www.globalresearch.ca/google-corporate-press-launch-attack-on-alternative-media/5557677> .

<sup>146</sup> See 2.4 of <http://www.itu.int/en/Lists/consultationJune2017/Attachments/4//CWG-Internet%202017-2.pdf>

<sup>147</sup> See the report at:

[http://www.un.org/ga/search/view\\_doc.asp?symbol=A/71/373](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> and

<http://news.sky.com/story/amber-rudd-only-has-google-meetings-planned-as-she-urges-web-extremism-crackdown-10969423> and

<https://www.bloomberg.com/news/articles/2017-07-10/australia-s-turnbull-urges-internet-providers-to-block-extremism>

<sup>148</sup> See for example

[http://www.cps.gov.uk/news/latest\\_news/cps\\_publishes\\_new\\_social\\_media\\_guidance\\_and\\_launches\\_hate\\_crime\\_consultation/](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/>

<sup>149</sup> 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](http://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/35/22)

<sup>150</sup> 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](http://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/35/22)

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.

## **1.8 Algorithms and Artificial Intelligence (AI)**

### **1.8.1 Ethical issues of networked automation, including driverless cars**

We reiterate and amplify comments made in our previous submissions to CWG-Internet.<sup>152</sup>

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.<sup>153</sup> 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<sup>154</sup>.

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.”<sup>155</sup> See also the discussion of algorithmic data processing and artificial intelligence presented under item 1 above.

At present, some actions have been proposed at the national level<sup>156</sup>, but there does not appear to be adequate consideration of these issues at the international level.

We recommend to invite UNESCO and UNICTRAL to study the ethical issues of networked automation, including driverless cars, which include ethical and legal aspects.<sup>157</sup> As a starting point, the study should

---

<sup>151</sup> See for example <https://www.theguardian.com/technology/2016/sep/09/facebook-deletes-norway-pms-post-napalm-girl-post-row>

<sup>152</sup> See 2.9 of <http://www.itu.int/en/Lists/consultationJune2017/Attachments/4//CWG-Internet%202017-2.pdf>

<sup>153</sup> <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML%2BCOMPARL%2BPE-582.443%2B01%2BDOC%2BPDF%2BV0//EN>

<sup>154</sup> <https://www.technologyreview.com/s/604087/the-dark-secret-at-the-heart-of-ai/>

<sup>155</sup> <http://arxiv.org/abs/1606.08813>

<sup>156</sup> <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML%2BCOMPARL%2BPE-582.443%2B01%2BDOC%2BPDF%2BV0//EN>

<sup>157</sup> 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

consider the IEEE Global Initiative for Ethical Considerations in Artificial Intelligence and Autonomous Systems. *Ethically Aligned Design: A Vision For Prioritizing Wellbeing With Artificial Intelligence And Autonomous Systems*, Version 1. IEEE, 2016.<sup>158</sup>

### 1.8.2 How to deal with induced job destruction and wealth concentration

We reiterate and amplify comments made in our previous submissions to CWG-Internet.<sup>159</sup>

Scholars have documented the reduction in employment that has already been caused by automation<sup>160</sup>. It is likely that this trend will be reinforced in the future.<sup>161</sup> 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.<sup>162</sup> And artificial intelligence can even result in the elimination of high-skilled jobs<sup>163</sup>, including creation of software<sup>164</sup>. These developments, including the so-called sharing economy, pose policy and regulatory challenges<sup>165</sup>, in particular for developing countries<sup>166</sup>. As the Internet Society puts

---

<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/>

<sup>158</sup> [http://standards.ieee.org/develop/indconn/ec/autonomous\\_systems.html](http://standards.ieee.org/develop/indconn/ec/autonomous_systems.html)

<sup>159</sup> See 2.10 of <http://www.itu.int/en/Lists/consultationJune2017/Attachments/4//CWG-Internet%202017-2.pdf>

<sup>160</sup> 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/>

<sup>161</sup> <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](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](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](http://unctad.org/en/PublicationsLibrary/ldc2016_en.pdf)

<sup>162</sup> 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>

<sup>163</sup> <https://www.technologyreview.com/s/603431/as-goldman-embraces-automation-even-the-masters-of-the-universe-are-threatened/>

<sup>164</sup> <https://www.technologyreview.com/s/603381/ai-software-learns-to-make-ai-software/>

<sup>165</sup> See for example p. 89 of GCIg. And the recent call for doing more to help globalization's losers by Mario Draghi, the president of 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:

the matter on page 35 of its 2017 Global Internet Report: Paths to Our Digital Future<sup>167</sup>: “The benefits of AI may also be unevenly distributed: for economies that rely on low-skilled labour, automation could challenge their competitive advantage in the global labour market and exacerbate local unemployment challenges, impacting economic development.” See also the discussion on page 66 ff. of the cited report.

Further, it has been observed that income inequality<sup>168</sup> is increasing in most countries, due at least in part to the deployment of ICTs<sup>169</sup>. 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<sup>170</sup>. 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

---

<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](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 “Artificial Intelligence and Robotics and Their Impact on the Workplace”, available at:

<https://www.ibanet.org/Article/NewDetail.aspx?ArticleUid=012a3473-007f-4519-827c-7da56d7e3509>

<sup>166</sup> 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](http://unctad.org/en/PublicationsLibrary/presspb2016d6_en.pdf)

<sup>167</sup> <https://future.internetsociety.org/wp-content/uploads/2017/09/2017-Internet-Society-Global-Internet-Report-Paths-to-Our-Digital-Future.pdf>

<sup>168</sup> 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/>

<sup>169</sup> See for example pp. 14, 20-21, and 118 ff. of the World Bank’s 2016 World Development Report (WDR-2016), titled “Digital Dividends”, available at:

<http://documents.worldbank.org/curated/en/896971468194972881/pdf/102725-PUB-Placement-PUBLIC.pdf>

<sup>170</sup> 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](https://en.wikipedia.org/wiki/Social_justice) ;

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

goals may erode social justice.<sup>171</sup> Further, the algorithms that are increasingly used to automate decisions such as granting home loans may perpetuate or even increase inequality and social injustice.<sup>172</sup>

At present, there does not appear to be adequate consideration of these issues at the international level, even if ILO<sup>173</sup> has recently started to address some of the issues.

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

## **2. Approaches and examples of good practices to promote the access and use of ICTs by SMEs, in developing and least-developed countries, particularly those owned/managed by women**

As noted above, access is a key issue. As stated in a recent study<sup>174</sup>:

... Citizens unable to access digital tools are too often confined to the lower or peripheral edge of the society for economic or geographic reasons, such as living in underserved areas without access to digital interaction. As a result of this inaccessibility, such groups are denied full involvement in mainstream economic, political, cultural, and social activities. This may also mean restricted access to or exclusion from critical services such as health, education, and other public services—and therefore limited opportunities for development.

If access to digital devices and access to connectivity (the Internet) has a critical impact on both social inclusion and our natural environment, we argue for positioning the infrastructure for digital social interaction as a resource commons. Therefore, citizens should decide collectively about the limits, congestion, management, and preservation of that infrastructure. This line of argumentation leads us to consider the governance of these resource systems as common property. Governance issues lead to considerations of human rights and the right of everyone to participate in the governance of the digital world, instead of just the private elite who design and control the fabric of public digital space.

---

<sup>171</sup> <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>

<sup>172</sup> <https://www.fordfoundation.org/ideas/equal-change-blog/posts/weapons-of-math-destruction-data-scientist-cathy-o-neil-on-how-unfair-algorithms-perpetuate-inequality/>

<sup>173</sup> <http://www.other-news.info/2017/04/humanity-and-social-justice-a-must-for-the-future-of-work-ryder/> and [http://ilo.org/global/topics/future-of-work/WCMS\\_569528/lang--en/index.htm](http://ilo.org/global/topics/future-of-work/WCMS_569528/lang--en/index.htm)

<sup>174</sup> <http://interactions.acm.org/archive/view/may-june-2017/sustainability-and-participation-in-the-digital-commons>

...

We argue that the future of societies around the world depends on accessibility and participation, that citizens must be able to fully engage in the governance of the digital, not only as mere users or consumers. The current model of unequal access to digital devices and connectivity is clearly unfair and unsustainable. Too few participate in the design and governance of the digital world, creating an elite of private interests. A minority of the world's population can enjoy the benefits of sleek devices and fast connectivity. Everyone is or will be influenced by the growing environmental impact of the digital world. If digitally excluded communities become peer-production actors, they will be able to build their own circular devices and sustainable network infrastructures, they will benefit from local reinvestment of surpluses, and they will have the opportunity to become active participants in the interactions of the design and governance of the common digital space.

The first step to address the issue is to recognize that access is a fundamental right and to take steps to provide access if market forces do not result in affordable access for all.

Specific approaches and examples of good practices to address these issues are given in the cited paper, and also in a recent paper by Michael Oghia<sup>175</sup>.

### **3. Available sources and mechanisms for measuring women's participation**

We have no comments on this issue.

### **4. Measures/policies to envisage to foster the role of women**

See above.

### **5. How to address gaps and the role of governments**

See above.

---

<sup>175</sup> <https://www.opendemocracy.net/hri/michael-j-oghia/internet-access-sustainability-and-citizen-participation-electricity-as-prerequisite>