

International Internet Public Policy Issues: Gaps Requiring Study

Richard Hill

Association for Proper Internet Governance¹

24 November 2016

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

Specific proposed recommendations are shown as text in boxes below. For convenience, the recommendations are numbered.

We refer to one of the outputs of previous meetings of the Working Group on Enhanced Cooperation, document E/CN.16/2015/CRP.2², Mapping of international Internet public policy issues, 17 April 2015.

That document states in Chapter 9, Concluding remarks:

The tension between the transborder nature of the Internet, on the one hand, and predominantly national regulations that govern public policy issues pertaining to the Internet, on the other, results into challenges for the implementation of regulation. Making diverse legislation more interoperable and aligning national laws with existing international instruments helps in overcoming these challenges. At the international level, this calls for strengthened cooperation, capacity building and sharing of information and best practices.

The review indicates that improvements could be made in respect of these gaps. At international level, strengthened coordination and collaboration across stakeholder groups will be critical in efforts to bridge them.

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

We note that many sections of the cited document identify areas where further study would be appropriate, in particular:

2.7 Net neutrality

2.8 Cloud

2.10 Internet of Things (IoT)

3.1 Cybersecurity

3.2 Cybercrime

¹ <http://www.apig.ch>

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

3.4 Cyber conflict

3.6 Encryption

3.7 Spam

4.1 Freedom of expression

4.2 Privacy and data protection

5.3 Copyright

5.5 Labour law

5.6 Intermediaries

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

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

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

1. The economic and social value of data and its processing

It is obvious that personal data has great value when it is collected on a mass scale and cross-referenced.³ Indeed, the monetization of personal data drives today's Internet services and the

³ See for example pp. vii and 2 of the GCIG report, available at:

http://ourinternet.org/sites/default/files/inline-files/GCIG_Final%20Report%20-%20USB.pdf . Henceforth referenced as "GCIG". See also 7.4 of

http://www.oecd-ilibrary.org/taxation/addressing-the-tax-challenges-of-the-digital-economy_9789264218789-en

provision of so-called free services such as search engines.⁴ Users should have greater control over the ways in which their data are used.⁵ All states should have comprehensive data protection legislation.⁶ The development of so-called “smart cities” might result in further erosion of individual control of personal data. As one journalist puts the matter⁷: “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” services⁸.

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”⁹ companies.

Further, mass-collected data (so-called “big data”) are increasingly being used, via computer algorithms, to make decisions that affect people’s lives, such as credit rating, availability of insurance, etc.¹⁰ The algorithms used are usually not made public so people’s lives are affected by computations made without their knowledge based on data that are often collected without their informed consent. It is important to avoid that “big data”, and the algorithmic treatment of personal data, do not result in increased inequality and increased social injustice which would threaten democracy.¹¹

⁴ <http://www.theatlantic.com/technology/archive/2014/08/advertising-is-the-internets-original-sin/376041/> and 7.4 of the cited OECD report.

⁵ See for example pp. 42, 106 and 113 of GCIIG. See also <http://www.internet-society.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

⁶ See for example p. 42 of GCIIG;

and section 5 of <http://www.itu.int/en/council/cwg-internet/Pages/display-feb2016.aspx?ListItemID=70>

⁷ <https://www.theguardian.com/cities/2014/dec/22/the-smartest-cities-rely-on-citizen-cunning-and-unglamorous-technology>

⁸ See “Stop rampant workplace surveillance” on p. 12 of:

<http://library.fes.de/pdf-files/id-moe/12797-20160930.pdf>

⁹ <http://thelongandshort.org/society/war-on-cash>

¹⁰ <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>

¹¹ 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/>

While some national legislators and/or courts have taken steps to strengthen citizens' rights to control the way their personal data are used¹², there does not appear to be adequate consideration of this issue at the international level.

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"¹³.

Regarding algorithmic use of data, what a UK parliamentary committee¹⁴ 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 as 'deep learning'. Though the capabilities of AI systems are currently narrow and specific, they are, nevertheless, starting to have transformational impacts on everyday life: from driverless cars and supercomputers that can assist doctors with medical diagnoses, to intelligent tutoring systems that can tailor lessons to meet a student's individual cognitive needs.

Such breakthroughs raise a host of social, ethical and legal questions. Our inquiry has highlighted several that require serious, ongoing consideration. These include taking steps to minimise bias being accidentally built into AI systems; ensuring that the decisions they make are transparent; and instigating methods that can verify that AI technology is operating as intended and that unwanted, or unpredictable, behaviours are not produced.

Similarly, the recommendations of a national artificial intelligence research and development strategic plan¹⁵ 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

¹² 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/>

¹³ <https://icdppc.org/wp-content/uploads/2015/02/Montreux-Declaration.pdf>

¹⁴ <http://www.publications.parliament.uk/pa/cm201617/cmselect/cmsctech/145/14502.htm>

¹⁵ https://www.nitrd.gov/news/national_ai_rd_strategic_plan.aspx

1. Consequently, it is proposed to recommend that UNCTAD¹⁶ and UNCITRAL be mandated 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) to make decisions, which issues include economic and legal aspects. In particular, UNCITRAL should be mandated to develop a model law, and possibly a treaty, on personal data protection¹⁷.

2. Takedown, filtering and blocking

An increasing number of states have implemented, or are proposing to implement, measures to restrict access to certain types of Internet content¹⁸, e.g. incitement to violence, gambling, copyright violation, or to take measures¹⁹ 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 speech²⁰, 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.

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.²¹

2. 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), it is proposed to recommend that IETF, ITU,

¹⁶ For a description of UNCTAD’s work addressing related issues, see:

<http://unctad14.org/EN/pages/NewsDetail.aspx?newsid=31>

¹⁷ 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>

¹⁸ See the report at:

http://www.un.org/ga/search/view_doc.asp?symbol=A/71/373 and the press release at:

<http://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=20717&LangID=E>

¹⁹ See for example

http://www.cps.gov.uk/news/latest_news/cps_publishes_new_social_media_guidance_and_launches_hate_crime_consultation/ ; and the summary article at:

<https://techcrunch.com/2016/10/12/ai-accountability-needs-action-now-say-uk-mps/>

²⁰ See the report cited above, A/71/373.

²¹ See for example <https://www.theguardian.com/technology/2016/sep/09/facebook-deletes-norway-pms-post-napalm-girl-post-row>

OHCHR, and UNESCO be mandated jointly to study the issue of takedown, filtering, and blocking, which includes technical, legal, and ethical aspects.

3. Intermediary liability

The issue of the extent to which Internet service providers, and other intermediaries such as providers of online video content, are or should be liable for allowing access to illegal material has been addressed by many national legislators.²²

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

3. Consequently, it is proposed to recommend that UNCITRAL be mandated to study the issue of intermediary liability, with a view to proposing a model law on the matter.

4. Privacy, encryption and prevention of inappropriate mass surveillance

Privacy is a fundamental right, and any violation of privacy must be limited to what is strictly necessary and proportionate in a democratic society.²³ Certain states practice mass surveillance that violates the right to privacy²⁴ (see for example A/HRC/31/64²⁵ and A/71/373²⁶).

Encryption is a method that can be used by individuals to guarantee the secrecy of their communications. Some states have called for limitations on the use of encryption, or for the implementation of technical measures to weaken encryption. Many commentators have pointed out that any weakening of encryption can be exploited by criminals and will likely have undesirable side effects (see for example paragraphs 42 ff. of A/HRC/29/32²⁷). Many commentators oppose state-attempts to compromise encryption.²⁸

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.²⁹

²² <https://cyberlaw.stanford.edu/our-work/projects/world-intermediary-liability-map-wilmap>

²³ See for example pp. vii, 32, 106 and 133 of GCIG.

²⁴ For an academic discussion, see <http://dx.doi.org/10.1080/23738871.2016.1228990>

²⁵ <http://ohchr.org/Documents/Issues/Privacy/A-HRC-31-64.doc>

²⁶ http://www.un.org/ga/search/view_doc.asp?symbol=A/71/373

²⁷ <https://documents-dds-ny.un.org/doc/UNDOC/GEN/G15/095/85/PDF/G1509585.pdf?OpenElement>

²⁸ See for example pp. vii, 106, and 113 of GCIG. See also <http://science.sciencemag.org/content/352/6292/1398> ; <http://www.internetsociety.org/policybriefs/encryption> ;

section 4 of <http://www.itu.int/en/council/cwg-internet/Pages/display-feb2016.aspx?ListItemID=70>

²⁹ See for example p. 66 of GCIG.

Secrecy of telecommunications is guaranteed by article 37 of the ITU Constitution. However, this provision appears to be out of date and to require modernization. In particular, restrictions must be placed on the collection and aggregation of meta-data.³⁰

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

4. Consequently, it is proposed to recommend that IETF, ISOC, ITU, and OHCHR be mandated to study the issues of privacy, encryption and prevention of inappropriate mass surveillance, which include technical, user education, and legal aspects.

5. Internet of Things (IoT)

In the current environment, it can be expected that networked devices (the so-called Internet of Things – IoT)³¹ will transmit data to manufacturers and service providers with little or no restrictions on the use of the data.³² The recipients of the data could then correlate the data and resell it, as is currently the case for data collected by so-called free services such as search engines. Further, national surveillance programs could acquire such data and use it to construct profiles of individuals.

Such uses of data that are collected automatically for a specific purpose could have wide-reaching and unforeseen consequences.³³

Further, interconnected devices may make decisions affecting daily life,³⁴ and this may call for the development of a regulatory framework to protect the interests of citizens.

In addition, the security risks posed by interconnected devices may require government actions.³⁵ For example, there may be a need to provide incentives to those who make interconnected devices to make them secure: such incentives might be penalties for failure to build-in adequate security. In this context, it is worth considering past experience with various devices, including electrical devices: they all have to conform to legal standards, all countries enforce compliance with such standards. It is not legitimate to claim that security and safety requirement stifle technological innovation. It must be recalled that the primary goal of private companies is to maximize profits. The purpose of regulation is to prevent profit-

³⁰ See p. 31 of GCIG.

³¹ A good overview of the technology, and the issues it raises, can be found at:

<http://www.internetsociety.org/doc/iot-overview>

³² See <https://www.theguardian.com/technology/2015/jul/15/internet-of-things-mass-surveillance> and the articles it references.

³³ See for example:

http://www.itu.int/en/ITU-T/Workshops-and-Seminars/01072016/Documents/S1P3_Corinna_Schmitt_v3.pdf ; see also the “weaponization of everything”, see p. 2 of GCIG.

³⁴ <http://policyreview.info/articles/analysis/governance-things-challenge-regulation-law>

³⁵ https://www.schneier.com/blog/archives/2016/07/real-world_secu.html and

<https://www.scribd.com/document/328854049/DDoS-Letter-to-Chairman-Wheeler#download> and

<https://www.euractiv.com/section/innovation-industry/news/commission-plans-cybersecurity-rules-for-internet-connected-machines/> and

<http://www.dailydot.com/layer8/bruce-schneier-internet-of-things/>

maximization from resulting in the production of dangerous products. Since IoT products will be interconnected, at least to some degree, chaos can ensue if the products are not sufficiently secure³⁶ (e.g. all medical systems fail to work). Thus it is important to ensure that the products are sufficiently secure for mass deployment.

This is not a theoretical consideration. Insufficiently insecure IoT devices have already been used to perpetrate massive denial of service attacks, and such attacks could be used to bring down critical infrastructures.³⁷ As one security manager put the matter³⁸: “In a relatively short time we've taken a system built to resist destruction by nuclear weapons and made it vulnerable to toasters.”

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

5. Consequently, it is proposed to recommend that ITU, UNCITRAL and UNESCO be mandated to study issues related to IoT (including security of IoT devices, use of data from IoT devices, decisions made by IoT devices, etc.), which include technical, legal, and ethical aspects (for a partial list of such aspects, see Recommendation ITU-T Y.3001: Future networks: Objectives and design goals³⁹). The studies should take into account Recommendation ITU-T Y.3013: Socio-economic assessment of future networks by tussle analysis⁴⁰.

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

Security experts have long recognized that lack of ICT security creates a negative externality.⁴¹ 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.⁴²

As the Global Internet Report 2016 of the Internet Society puts the matter⁴³:

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

³⁶ A particularly frightening scenario is presented at:

<https://www.schneier.com/blog/archives/2016/11/self-propagatin.html>

³⁷ See <http://hothardware.com/news/latest-iot-ddos-attack-dwarfs-krebs-takedown-at-nearly-1-terabyte-per-second>

<http://hothardware.com/news/your-iot-device-could-be-part-of-a-ddos-botnet-how-to-shut-it-down>

https://www.schneier.com/blog/archives/2016/09/someone_is_lear.html

³⁸ Jeff Jarmoc, head of security for global business service Salesforce, quoted in the excellent summary article at:

<http://www.bbc.com/news/technology-37738823>

³⁹ <https://www.itu.int/rec/T-REC-Y.3001-201105-I>

⁴⁰ <http://www.itu.int/rec/T-REC-Y.3013-201408-I/en>

⁴¹ 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/>

⁴² See also pp. vii and 66 of GCIG.

⁴³ See p. 18 of the cited Global Internet Report 2016.

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.

As noted above, the externalities arising from lack of security are exacerbated by the Internet of Things (IoT)⁴⁴. As a well known security expert puts the matter⁴⁵: “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.”

While some national authorities are taking some measures⁴⁶, at present, there does not appear to be adequate consideration of these issues at either the national or international levels.

6. Consequently, it is proposed to recommend that IETF, ISOC, ITU, UNCITRAL, and UNCTAD be mandated 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.

7. Ethical issues of networked automation, including driverless cars

More and more aspects of daily life are controlled by automated devices, and in the near future automated devices will provide many services that are today provided manually, such as transportation. Automated devices will have to make choices and decisions.⁴⁷ It is important to ensure that the choices and decisions comply with our ethical values. 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.”⁴⁸ See also the discussion of algorithmic data processing and artificial intelligence presented under item 1 above.

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

⁴⁴ See p. 107 of the cited Global Internet Report 2016.

⁴⁵ https://www.schneier.com/blog/archives/2016/07/real-world_secu.html

⁴⁶ For example, for cybersecurity for motor vehicles, see:

http://www.nhtsa.gov/About-NHTSA/Press-Releases/nhtsa_cybersecurity_best_practices_10242016 .

For a general approach see Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, at:

<http://eur-lex.europa.eu/legal->

content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC

⁴⁷ <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML%2BCOMPARI%2BPE-582.443%2B01%2BDOC%2BPDF%2BV0//EN>

⁴⁸ <http://arxiv.org/abs/1606.08813>

7. Consequently, it is proposed to recommend that UNESCO and UNICTRAL be mandated to study the ethical issues of networked automation, including driverless cars, which include ethical and legal aspects.

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

Scholars have documented the reduction in employment that has already been caused by automation. It is likely that this trend will be reinforced in the future.⁴⁹ 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.⁵⁰ These developments, including the so-called sharing economy, pose policy and regulatory challenges.⁵¹

Further, it has been observed that income inequality is increasing in most countries, due at least in part to the deployment of ICTs. 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 justice⁵². Indeed, it has been posited that the small number of individuals who control the wealth generated by dominant platforms (see below) may be using that wealth to further particular economic and political goals, and that such goals may erode social justice.⁵³ Further, the algorithms that are increasingly used to automate decisions such as granting home loans may perpetuate or even increase inequality and social injustice.⁵⁴

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

⁴⁹ <http://robertmchesney.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

⁵⁰ 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/> ; and <https://www.technologyreview.com/s/602489/learning-to-prosper-in-a-factory-town/>

⁵¹ 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: <https://www.ft.com/content/ab3e3b3e-79a9-11e6-97ae-647294649b28>

⁵² 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

⁵³ <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>

⁵⁴ <https://www.fordfoundation.org/ideas/equals-change-blog/posts/weapons-of-math-destruction-data-scientist-cathy-o-neil-on-how-unfair-algorithms-perpetuate-inequality/>

8. Consequently, it is proposed to recommend that ILO and UNCTAD be mandated to study the issues of induced job destruction, wealth concentration, and the impact of algorithms on social justice and that UNCTAD compile, and coordinate the studies made by other agencies such as OECD, World Bank, IMF.

9. How to deal with platform dominance

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

But if the dominance is due to economies of scale and network effects, then a situation akin to a natural monopoly⁵⁵ might arise, there might be abuse of dominant market power⁵⁶, and regulatory intervention is required⁵⁷. Appropriate regulatory intervention might be different from that arising under competition or anti-trust policies.⁵⁸ As one commentator puts the matter⁵⁹ (his text starts with a citation):

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

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

⁵⁵ https://en.wikipedia.org/wiki/Natural_monopoly

⁵⁶ <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

⁵⁷ 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.

⁵⁸ <https://www.competitionpolicyinternational.com/let-the-right-one-win-policy-lessons-from-the-new-economics-of-platforms/>

⁵⁹ 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>

As noted above, the dominance of certain platforms raises issues related to freedom of speech, because some platforms apply strict rules of their own to censor certain types of content⁶⁰, and, for many users, there are no real alternatives to dominant platforms⁶¹.

As *The Economist* puts the matter⁶²:

“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.”

National authorities in a number of countries have undertaken investigations,⁶³ and even imposed measures,⁶⁴ 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.”⁶⁵

However, it does not appear that there is an adequate platform for exchanging national experiences regarding such matters.⁶⁶

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.⁶⁷

⁶⁰ See for example <https://www.theguardian.com/technology/2016/sep/09/facebook-deletes-norway-pms-post-napalm-girl-post-row>

⁶¹ <https://www.theguardian.com/technology/2016/nov/17/google-suspends-customer-accounts-for-reselling-pixel-phones>

⁶² <http://www.economist.com/news/leaders/21707210-rise-corporate-colossus-threatens-both-competition-and-legitimacy-business>

⁶³ See for example http://europa.eu/rapid/press-release_IP-16-1492_en.htm ;
http://europa.eu/rapid/press-release_IP-16-2532_en.htm and
http://europa.eu/rapid/press-release_IP-15-5166_en.htm ;

a more general approach is described at:

<http://www.accc.gov.au/media-release/accc-to-undertake-market-study-of-the-communications-sector>

⁶⁴ See for example http://www.autoritedelaconcurrence.fr/user/standard.php?id_rub=606&id_article=2534

⁶⁵ <http://www.cnet.com/news/senator-warren-says-apple-google-and-amazon-have-too-much-power/>

⁶⁶ 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>

9.1 Consequently, it is proposed that UNCTAD be mandated to study the economic and market issues related to platform dominance, and to facilitate the exchange of information on national 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.⁶⁸

9.2 Consequently, it is proposed to recommend that the Inter-Parliamentary Union (IPU) and the UN HCHR be mandated to study the potential effects of platform dominance on elections and democracy.

10. How to deal with embedded software

More and more devices used in ordinary life, including in particular automobiles, depend more and more on software. Software is protected by copyright law. Thus users who buy a device have increasingly less control over the device, because they cannot change the software controls the device. This raises significant policy issues.⁶⁹ In fact, attempts to change the software may be criminal acts in some countries.

This situation may result in a significant shift of market power away from consumers, thus reducing competition. At present, there does not appear to be adequate consideration of these issues at the international level.

10. Consequently, it is proposed to recommend that UNCTAD and WIPO be mandated to study the issues related to embedded software, which include economic and legal issues.

⁶⁷ See for example pp. 12 and 13 of <http://library.fes.de/pdf-files/id-moe/12797-20160930.pdf> and <https://www.theguardian.com/technology/2016/oct/28/uber-uk-tribunal-self-employed-status> .

A more general discussion of various issues arising out of platform dominance is at:

<http://www.alainet.org/en/articulo/181307>

⁶⁸ <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> ;

for a possible impact on free speech, see:

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

⁶⁹ <http://copyright.gov/policy/software/>