Response to NTIA Docket No. 170105023-7023-01, RIN: 0660-XC033 The Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things

Richard Hill
Association for Proper Internet Governance[1]

15 January 2017

This submission responds to the cited request for public comments.

As a preliminary matter, we note that the "things" that comprise the Internet of Things, whether hardware or software, are produced around the world and marketed internationally. So no national solutions or policies are likely to be effective: international coordination is required to address the issues outlined in NTIA's Green Paper[2].

Issues related specifically to IoT are addressed in section 3 below, and the related security issues are addressed in section 4.

Before turning to IoT specifically, we discuss in sections 1 and 2 issues related to personal data and to privacy and encryption.

In sections 5, 6, and 7 we discuss the ethical issues arising out of IoT, how to deal with induced job destruction, and how to deal with embedded software.

Specific actions that governments, including the US government, should take to address the issues are proposed in paragraphs surrounded by a box, at the end of each section below.

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 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]

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

[2] https://www.ntia.doc.gov/other-publication/2017/green-paper-fostering-advancement-internet-things

[3] See for example pp. vii and 2 of the Report of the Global Commission on Internet Governance, available at: http://ourinternet.org/sites/default/files/inline-files/GCIG_Final%20Report%20-%20USB.pdf . Henceforth referenced as "GCIG". See also 7.4 of http://www.oecd-ilibrary.org/taxation/addressing-the-tax-challenges-of-the-digital-economy_9789264218789-en ; and http://www.other-news.info/2016/12/they-have-right-now-another-you/

[4] 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/

[5] See for example pp. 42, 106 and 113 of GCIG. See also http://www.internetsociety.org/policybriefs/privacy ; and http://www.faz.net/aktuell/feuilleton/debatten/the-digital-debate/shoshana-zuboff-secrets-of-surveillance-capitalism-14103616.html ; and

The development of so-called “smart cities” might result in further erosion of individual control of personal data. As one journalist puts the matter[7]: “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[8].

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]

While some national legislators and/or courts have taken steps to strengthen citizens’ rights to control the way their personal data are used[12], there does not appear to be adequate consideration of this issue at the international level.[13]

http://ec.europa.eu/commission/2014-2019/oettinger/announcements/speech-conference-building-european-data-economy_en

[6] 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

[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/

[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] 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

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" [14].

Regarding algorithmic use of data, what a UK parliamentary committee[15] 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 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[16] 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

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

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

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

Consequently, it is proposed to recommend that UNCTAD[17] and UNCITRAL be requested to study the issues related to the economic and social value or data, in particular "big data" and the increasing use of algorithms (including artificial intelligence) 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 protection[18].

2. 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.[19] Certain states practice mass surveillance that violates the right to privacy[20] (see for example A/HRC/31/64[21] and A/71/373[22] and European Court of Justice judgment[23] ECLI:EU:C:2016:970 of 21 December 2016).

Encryption is a method that can be used by individuals to guarantee the secrecy of their communications. Some states have called for limitations on the use of encryption, or for the implementation of technical measures to weaken encryption. Many commentators have pointed out that any weakening of encryption can be exploited by criminals and will likely have undesirable side effects (see for example paragraphs 42 ff. of A/HRC/29/32[24]). Many commentators oppose state-attempts to compromise encryption.[25] The 2016 UNESCO Report "Human rights and encryption" also points out that attempts to limit the use of encryption, or to weaken encryption methods, may impinge on freedom of expression and the right to privacy.[26]

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

[17] For a description of UNCTAD's work addressing related issues, see: http://unctad14.org/EN/pages/NewsDetail.aspx?newsid=31

[18] 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

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

[20] For an academic discussion, see http://dx.doi.org/10.1080/23738871.2016.1228990

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

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

[23] 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

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

[25] 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

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

general need to increase awareness of ways and means for end-users to improve the security of the systems they use.[27]

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.[28]

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

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

3. Internet of Things (IoT)

In the current environment, it can be expected that networked devices (the so-called Internet of Things – IoT)[29] will transmit data to manufacturers and service providers with little or no restrictions on the use of the data. [30] 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.[31]

Further, interconnected devices may make decisions affecting daily life,[32] 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.[33] 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,

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

[28] See p. 31 of GCIG.

[29] A good overview of the technology, and the issues it raises, can be found at: http://www.internetsociety.org/doc/iot-overview

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

[31] 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.

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

[33] 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/

it is worth considering past experience with various devices, including electrical devices: they all have to conform to legal standards, all countries enforce compliance with such standards. It is not legitimate to claim that security and safety requirement stifle technological innovation. It must be recalled that the primary goal of private companies is to maximize profits. The purpose of regulation is to prevent profit-maximization from resulting in the production of dangerous products. Since IoT products will be interconnected, at least to some degree, chaos can ensue if the products are not sufficiently secure[34] (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.[35] As one security manager put the matter[36]: "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.

Consequently, it is proposed to recommend that ITU, UNCITRAL and UNESCO be requested to study issues related to IoT (including security of IoT devices, use of data from IoT devices, decisions made by IoT devices, etc.), which include technical, legal, and ethical aspects (for a partial list of such aspects, see Recommendation ITU-T Y.3001: Future networks: Objectives and design goals[37]). The studies should take into account Recommendation ITU-T Y.3013: Socio-economic assessment of future networks by tussle analysis[38].

4. 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.[39] 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.[40]

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

[35] 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

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

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

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

[39] 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/

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

As the Global Internet Report 2016 of the Internet Society puts the matter[41]:

> 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.

As noted above, the externalities arising from lack of security are exacerbated by the Internet of Things (IoT)[42]. As a well known security expert puts the matter[43]: "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 measures[44], at present, there does not appear to be adequate consideration of these issues at either the national or international levels.

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

5. 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.[45] 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

[41] See p. 18 of the cited Global Internet Report 2016.
[42] See p. 107 of the cited Global Internet Report 2016.
[43] https://www.schneier.com/blog/archives/2016/07/real-world_secu.html
[44] 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
[45] http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML%2BCOMPARL%2BPE-582.443%2B01%2BDOC%2BPDF%2BV0//EN

made about them."[46] See also the discussion of algorithmic data processing and artificial intelligence presented under item 1 above.

At present, some action have been proposed at the national level[47], but there does not appear to be adequate consideration of these issues at the international level.

Consequently, it is proposed to recommend that UNESCO and UNICTRAL be requested to study the ethical issues of networked automation, including driverless cars, which include ethical and legal aspects.[48]

6. 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 justice[52]. 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

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

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

[48] A commission of the European Parliament has "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.

[49] 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 .
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

[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/ ; 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/

[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 if the European Central Bank, Donald Tusk, the president of the European Council, and Christine Lagarde, the head of the International Monetary Fund, reported in the Financial Times: https://www.ft.com/content/ab3e3b3e-79a9-11e6-97ae-647294649b28

[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

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.

Consequently, it is proposed to recommend that ILO and UNCTAD be requested 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.

7. 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.[55] 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.

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

[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/

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