

**Submission to the Expert workshop on the right to privacy in the digital age
Geneve, 19-20 February 2018**

Richard Hill, Association for Proper Internet Governance¹

This paper discusses the following issues and makes specific recommendations:

1. The economic and social value of data and its processing is one of the key issues of our times. Consequently, it is important to understand the implications and to agree international binding norms on privacy and data protection.
2. Mass surveillance must be curtailed and pervasive strong encryption must be implemented.
3. Measures must be taken to address the dominance of certain Internet platforms, since uncontrolled dominance threatens privacy and may even undermine democracy itself.
4. Norms regarding privacy and data protection must not be negotiated in trade-related forums such as the World Trade Organization or plurilateral free trade agreements.

What follows is excerpted from our submission to the Working Group on Enhanced Cooperation, see:

http://unctad.org/meetings/en/Contribution/WGEC_m5_RevRecom_RichardHill_en.pdf

and

<http://www.apig.ch/Gaps%20r9%20clean.pdf>

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.² An excellent discussion of this topic, with numerous references, is give in pp. 9 ff. of Third World Network, Briefing no. 3 for the World Trade Organization 11th Ministerial Conference, Buenos Aires, 10-13 December 2017, at: <http://www.twn.my/MC11/briefings/BP3.pdf> .

¹ <http://www.apig.ch>

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

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

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

; and <http://www.other-news.info/2016/12/they-have-right-now-another-you/> ; and the study of data brokers at:

<https://www.opensocietyfoundations.org/sites/default/files/data-brokers-in-an-open-society-20161121.pdf> ;

<https://www.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> and

[facebook](http://www.theguardian.com/world/2017/aug/23/silicon-valley-big-data-extraction-amazon-whole-foods-facebook) and

pages 6-7 of UNCTAD's *Information Economy Report 2017: Digitalization, Trade and Development*,

<http://unctad.org/en/pages/PublicationWebflyer.aspx?publicationid=1872> and

<http://www.autoritedelaconcurrence.fr/doc/reportcompetitionlawanddatafinal.pdf> and

<https://www.diplomacy.edu/blog/2018predictions#1>

Indeed, the monetization of personal data drives today's Internet services and the provision of so-called free services such as search engines.³ These developments have significant implications, in particular for developing countries.⁴ Users should have greater control over the ways in which their data are used.⁵ 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.⁶ 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 form⁷. The Internet Society recommends the following⁸: "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."⁹

The following joke¹⁰ well illustrates what is happening:

³ <http://www.theatlantic.com/technology/archive/2014/08/advertising-is-the-internets-original-sin/376041/> and 7.4 of the cited OECD report; and <http://www.other-news.info/2016/12/they-have-right-now-another-you/> and <https://www.internetsociety.org/blog/public-policy/2017/03/my-data-your-business>

⁴ <http://twm.my/title2/resurgence/2017/319-320/cover03.htm> ; see also page 12 of UNCTAD's *Information Economy Report 2017: Digitalization, Trade and Development*, <http://unctad.org/en/pages/PublicationWebflyer.aspx?publicationid=1872>

⁵ 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 and

<http://webfoundation.org/2017/03/web-turns-28-letter/> and

https://ec.europa.eu/futurium/en/system/files/ged/ec_ngi_final_report_1.pdf and

<https://www.internetsociety.org/blog/public-policy/2017/03/my-data-your-business> and

https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2017/17-03-14_Opinion_Digital_Content_EN.pdf and

<http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+COMPARL+PE-592.279+01+DOC+PDF+V0//EN&language=EN> and

<https://www.reuters.com/article/us-facebook-spain-fine/facebook-fined-1-2-million-euros-by-spanish-data-watchdog-idUSKCN1BM1OU> and

<https://www.economist.com/news/leaders/21735021-dominance-google-facebook-and-amazon-bad-consumers-and-competition-how-tame>

⁶ <https://www.theguardian.com/technology/2017/jun/04/surge-pricing-comes-to-the-supermarket-dynamic-personal-data>

⁷ <https://gizmodo.com/before-you-hit-submit-this-company-has-already-logge-1795906081?null>

⁸ 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>

⁹ 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://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)

; see also the good discussion in paragraphs 21-35, 88-97, and 103-112 of the 19 October 2017 Report of the Special Rapporteur on Privacy, document A/72/43103,

http://www.ohchr.org/Documents/Issues/Privacy/A-72-43103_EN.docx

CALLER: Is this Gordon's Pizza?
GOOGLE: No sir, it's Google Pizza.
CALLER: I must have dialed a wrong number. Sorry.
GOOGLE: No sir, Google bought Gordon's Pizza last month.
CALLER: OK. I would like to order a pizza.
GOOGLE: Do you want your usual, sir?
CALLER: My usual? You know me?
GOOGLE: According to our caller ID data sheet, the last 12 times you called you ordered an extra-large pizza with three cheeses, sausage, pepperoni, mushrooms and meatballs on a thick crust.
CALLER: OK! That's what I want ...
GOOGLE: May I suggest that this time you order a pizza with ricotta, arugula, sun-dried tomatoes and olives on a whole wheat gluten free thin crust?
CALLER: What? I detest vegetables.
GOOGLE: Your cholesterol is not good, sir.
CALLER: How the hell do you know?
GOOGLE: Well, we cross-referenced your home phone number with your medical records. We have the result of your blood tests for the last 7 years.
CALLER: Okay, but I do not want your rotten vegetable pizza! I already take medication for my cholesterol.
GOOGLE: Excuse me sir, but you have not taken your medication regularly. According to our database, you only purchased a box of 30 cholesterol tablets once, at Drug RX Network, 4 months ago.
CALLER: I bought more from another drugstore.
GOOGLE: That doesn't show on your credit card statement.
CALLER: I paid in cash.
GOOGLE: But you did not withdraw enough cash according to your bank statement.
CALLER: I have other sources of cash.
GOOGLE: That doesn't show on your last tax return unless you bought them using an undeclared income source, which is against the law.
CALLER: WHAT THE HELL?
GOOGLE: I'm sorry, sir, we use such information only with the sole intention of helping you.
CALLER: Enough already! I'm sick to death of Google, Facebook, Twitter, WhatsApp and all the others. I'm going to an island without internet, cable TV, where there is no cell phone service and no one to watch me or spy on me
GOOGLE: I understand sir, but you need to renew your passport first. It expired 6 weeks ago...

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"¹¹ 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

¹⁰ <http://www.jokesoftheday.net/joke-Google-s-pizza/2017051897>

¹¹ <http://www.pnas.org/content/110/15/5802.full#aff-1>

mortgage for their home¹². In fact, big data is already being used in ways that could lead to social control, see:

<https://www.wired.com/story/age-of-social-credit/>

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.¹³

The Indian government has published a White Paper which provides a comprehensive analysis of the issues and data protection legislation adopted in various jurisdictions, see:

http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_171127_final_v2.pdf

All states should have comprehensive data protection legislation.¹⁴ The development of so-called “smart cities” might result in further erosion of individual control of personal data. As one journalist puts the matter¹⁵: “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” services¹⁶.

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”¹⁷ companies.

Further, mass-collected data (so-called “big data”¹⁸) are increasingly being used, via computer algorithms, to make decisions that affect people’s lives, such as credit rating, availability of insurance,

¹² <https://www.theguardian.com/commentisfree/2017/jun/18/google-not-gchq--truly-chilling-spy-network> and <https://www.socialcooling.com/>

¹³ See document 2017/0003(COD) of 9 June 2017, available at: <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-%2f%2fEP%2f%2fNONGML%2bCOMPARL%2bPE-606.011%2b01%2bDOC%2bPDF%2bV0%2f%2fEN>

¹⁴ 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

¹⁵ <https://www.theguardian.com/cities/2014/dec/22/the-smartest-cities-rely-on-citizen-cunning-and-unglamorous-technology>

¹⁶ See “Stop rampant workplace surveillance” on p. 12 of: <http://library.fes.de/pdf-files/id-moe/12797-20160930.pdf>

¹⁷ <http://thelongandshort.org/society/war-on-cash>

¹⁸ An excellent overview of the topic is provided in the May 2014 report commissioned by then-US President Obama, “Big Data: Seizing Opportunities, Preserving Values”, available at: https://bigdatawg.nist.gov/pdf/big_data_privacy_report_may_1_2014.pdf. An academic analysis of the social and public interest aspects of big data is given in Taylor, L., Floridi, L., van der Sloot, B. eds. (2017) *Group Privacy: new challenges of data technologies*. Dordrecht: Springer, available at:

etc.¹⁹ 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. An excellent analysis of the human rights dimensions of algorithms is found in Council of Europe document MSI-NET(2016)06²⁰, 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 inequality²¹ and increased social injustice²² which would threaten democracy.²³ 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.²⁴ See also the discussion on pp. 75 ff. of the 2017 Internet Society Global Internet Report: Paths to Our Digital Future²⁵.

As learned scholars have put the matter²⁶:

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.

<https://www.stiftung-nv.de/sites/default/files/group-privacy-2017-authors-draft-manuscript.pdf> ;

see also the analysis and recommendations at:

<https://medium.com/@AINowInstitute/the-10-top-recommendations-for-the-ai-field-in-2017-b3253624a7>

¹⁹ <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>

²⁰ <https://rm.coe.int/16806a7ccc>

²¹ <https://inequality.org/facts/income-inequality/> and

<http://wir2018.wid.world/files/download/wir2018-summary-english.pdf>

²² Even a well-known business publication has recognized that there is a need to address the issue of social equality, see:

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

see also pp. 13 and 57 of https://bigdatawg.nist.gov/pdf/big_data_privacy_report_may_1_2014.pdf

²³ See Cathy O'Neil, *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*, Crown Publishing, 2016; article at:

<https://www.wired.com/2016/10/big-data-algorithms-manipulating-us/>

²⁴ http://citris-uc.org/wp-content/uploads/2017/07/Inclusive-AI_CITRIS_2017.pdf

²⁵ <https://future.internetsociety.org/wp-content/uploads/2017/09/2017-Internet-Society-Global-Internet-Report-Paths-to-Our-Digital-Future.pdf>

²⁶ 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>

Another way of putting it is to note that the use of data is an extractive industry analogous to the mining and oil industries: “No reasonable person would let the mining industry unilaterally decide how to extract and refine a resource, or where to build its mines. Yet somehow we let the tech industry make all these decisions [regarding data] and more, with practically no public oversight. A company that yanks copper out of an earth that belongs to everyone should be governed in everyone’s interest. So should a company that yanks data out of every crevice of our collective lives.”²⁷

Control of large amounts of data may lead to dominant positions that impeded competition²⁸. 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.”²⁹

While some national legislators and/or courts have taken steps to strengthen citizens’ rights to control the way their personal data are used³⁰, to consider product liability issues related to data³¹, and to consider the impact of big data with respect to prohibitions of discrimination in hiring³², there does not appear to be adequate consideration of this issue at the international level.³³ Yet failure to address the issue at the international level can have negative consequences, including for trade. As UNCTAD puts the matter³⁴:

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.

²⁷ <https://www.theguardian.com/world/2017/aug/23/silicon-valley-big-data-extraction-amazon-whole-foods-facebook>

²⁸ <https://www.wired.com/story/ai-and-enormous-data-could-make-tech-giants-harder-to-topple/>

²⁹ <https://www.theguardian.com/commentisfree/2016/dec/04/data-populists-must-seize-information-for-benefit-of-all-evgeny-morozov>

³⁰ 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/>

³¹ <http://www.wablegal.com/european-commission-publishes-roadmap-future-proof-eu-product-liability-directive/>

³² <https://www.eeoc.gov/eeoc/meetings/10-13-16/index.cfm>

³³ Indeed, a group of scholars has called for the creation of a charter of digital rights, see:

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

See also the UNCTAD study at: http://unctad.org/en/PublicationsLibrary/dtlstict2016d1_en.pdf ; and

<http://www.economist.com/news/leaders/21721656-data-economy-demands-new-approach-antitrust-rules-worlds-most-valuable-resource> ; and the balanced discussion in pp. 93-95 of UNCTAD’s *Information Economy Report 2017: Digitalization, Trade and Development*,

<http://unctad.org/en/pages/PublicationWebflyer.aspx?publicationid=1872>

³⁴ *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

...

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”³⁵.

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 age³⁶. 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.³⁷ We also note that the BRICS Leaders Xiamen Declaration³⁸ (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 committee³⁹ 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

³⁵ <https://icdppc.org/wp-content/uploads/2015/02/Montreux-Declaration.pdf>

³⁶ http://www.un.org/ga/search/view_doc.asp?symbol=A/HRC/34/L.7/Rev.1

³⁷ See 5(f) and 5(k) of the cited Resolution

³⁸ Available at: http://www.mea.gov.in/Uploads/PublicationDocs/28912_XiamenDeclaratoin.pdf

³⁹ <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.

A more detailed discussion is given in paragraphs 5-76 of the 19 October 2017 Report of the Special Rapporteur on Privacy.⁴⁰

The recommendations of a national artificial intelligence research and development strategic plan⁴¹ can also 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.⁴²

And experts speaking at a conference⁴³ on Artificial Intelligence hosted by the ITU raised many of the issues raised in this paper⁴⁴, as did experts at the AI Now public symposium, hosted by the White House and New York University's Information Law Institute, July 7th, 2016⁴⁵, as did a report by the UK Royal Society⁴⁶, as did the Internet Society in pages 31 ff. of its 2017 Global Internet Report: Paths to Our Digital Future⁴⁷. 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.aan6080⁴⁸. See also pages 4-5 of UNCTAD's

⁴⁰ Document A/72/43103, http://www.ohchr.org/Documents/Issues/Privacy/A-72-43103_EN.docx

⁴¹ https://www.nitrd.gov/news/national_ai_rd_strategic_plan.aspx

⁴² 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>

⁴³ <http://www.itu.int/en/ITU-T/AI/Pages/201706-default.aspx>. The report of the event is at:

<https://www.slideshare.net/ITU/ai-for-good-global-summit-2017-report>

⁴⁴ 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/>

⁴⁵ https://artificialintelligenow.com/media/documents/AINowSummaryReport_3_RpmwKHu.pdf

⁴⁶ <https://royalsociety.org/topics-policy/projects/machine-learning/>

⁴⁷ <https://future.internetsociety.org/wp-content/uploads/2017/09/2017-Internet-Society-Global-Internet-Report-Paths-to-Our-Digital-Future.pdf>

⁴⁸ <http://robotics.sciencemag.org/content/2/6/ean6080>

*Information Economy Report 2017: Digitalization, Trade and Development*⁴⁹ and one expert's⁵⁰ predictions for 2018.

We recommend to invite UNCTAD⁵¹ 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 intelligence⁵²) to make decisions⁵³, which issues include economic and legal aspects. In particular, UNCITRAL should be mandated to develop model laws, and possibly treaties, on personal data protection⁵⁴, algorithmic transparency and accountability⁵⁵, and artificial intelligence⁵⁶; UNCTAD should

⁴⁹ <http://unctad.org/en/pages/PublicationWebflyer.aspx?publicationid=1872>

⁵⁰ <https://www.diplomacy.edu/blog/2018predictions#5>

⁵¹ 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 ; we also note the newly created Intergovernmental Group of Experts on E-Commerce, see:

<http://unctad.org/en/Pages/MeetingDetails.aspx?meetingid=1437>

⁵² For a discussion of some of the issues related to AI, see:

https://www.wired.com/2017/02/ai-threat-isnt-skynet-end-middle-class/?mbid=nl_21017_p3&CNDID=42693809 and

<https://www.technologyreview.com/s/608248/biased-algorithms-are-everywhere-and-no-one-seems-to-care/> ;

and <https://www.technologyreview.com/s/607955/inspecting-algorithms-for-bias/> ; and

<https://blogs.microsoft.com/blog/2018/01/17/future-computed-artificial-intelligence-role-society/> ;

a good discussion of the issues and some suggestions for how to address them is found at:

<https://www.internetsociety.org/doc/artificial-intelligence-and-machine-learning-policy-paper>

⁵³ 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>

⁵⁴ 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.3600-201511-1/en> ; 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 ; the core principles on page 95 of UNCTAD's *Information Economy Report 2017: Digitalization, Trade and Development*,

<http://unctad.org/en/pages/PublicationWebflyer.aspx?publicationid=1872> ;

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)

; and the key principles found in Section V of the Indian White Paper (p. 214 of the PDF file, p. 204 of the document) available at:

http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_171127_final_v2.pdf ;

it should also consider the “Guidelines for the Regulation of Computerized Personal Data Files” adopted by the UN General Assembly resolution 45/95 of 14 December 1990; the Guidelines are at:

<http://www.refworld.org/pdfid/3ddcafaac.pdf> ;

the Resolution is at: <http://www.un.org/documents/ga/res/45/a45r095.htm> .

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> ; and it could also

consider the provisions in Chapter II of the African Union Convention on Cyber Security and Personal Data

be mandated to develop a study on the taxation of robots⁵⁷; and the UN Conference on Disarmament should consider taking measures with respect to lethal autonomous weapons⁵⁸.

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.⁵⁹ Certain states practice mass surveillance that violates the right to privacy⁶⁰ (see for example A/HRC/31/64⁶¹, A/71/373⁶², A/HRC/34/60⁶³ and European Court of Justice judgment⁶⁴ 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.⁶⁵ The UN Human Rights Council Special Rapporteur on the right to privacy stated that he had “identified a serious obstacle to privacy in that there is a vacuum in international law in surveillance and privacy in cyberspace. ... It is not only the lack of substantive rules which are an obstacle to privacy promotion and protection, but also one of

Protection, available at:

https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf; and the “Top 10 Principles for Workers’ Data Privacy and Protection” published by UNI Global Union, at: http://www.thefutureworldofwork.org/media/35421/uni_workers_data_protection.pdf.

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>.

⁵⁵ 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

⁵⁶ 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/>. It should take into account the “Top 10 Principles for Ethical Artificial Intelligence” published by UNI Global Union, at:

http://www.thefutureworldofwork.org/media/35420/uni_ethical_ai.pdf.

⁵⁷ <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>

⁵⁸ 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)

⁵⁹ 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)

⁶⁰ 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>

⁶¹ <http://ohchr.org/Documents/Issues/Privacy/A-HRC-31-64.doc>

⁶² http://www.un.org/ga/search/view_doc.asp?symbol=A/71/373

⁶³ 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.

⁶⁴ <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>

⁶⁵ 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

adequate mechanisms.”⁶⁶ He also stated that the UN should discuss and adopt a new instrument to protect privacy rights.⁶⁷

As UNCTAD puts the matter⁶⁸:

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 age⁶⁹. That resolution recalls that States should ensure that any interference with the right to privacy is consistent with the principles of legality, necessity and proportionality.⁷⁰ Even a well-known business publication has recognized that privacy is a pressing issue⁷¹. 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.⁷²

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.”⁷³

It appears to us that this decision and questions⁷⁴ 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

⁶⁶ Paragraph 4 of the 19 October 2017 Report of the Special Rapporteur on Privacy, document A/72/43103, http://www.ohchr.org/Documents/Issues/Privacy/A-72-43103_EN.docx

⁶⁷ Paragraph 5 of the cited report.

⁶⁸ *Data protection regulations and international data flows: Implications for trade and development*, p. 66, available at: http://unctad.org/en/PublicationsLibrary/dt1stict2016d1_en.pdf

⁶⁹ http://www.un.org/ga/search/view_doc.asp?symbol=A/HRC/34/L.7/Rev.1

⁷⁰ See 2 of the cited HRC Resolution

⁷¹ <http://www.economist.com/news/briefing/21721634-how-it-shaping-up-data-giving-rise-new-economy>

⁷² <https://www.internetsociety.org/doc/issue-paper-asia-pacific-bureau-%E2%80%93-online-privacy>

⁷³ <https://www.whitehouse.gov/the-press-office/2017/01/25/presidential-executive-order-enhancing-public-safety-interior-united>

⁷⁴ See for example: <http://www.sophieintveld.eu/letter-to-eu-commission-what-impact-has-trump-decisions-on-privacy-shield-and-umbrella-agreement/>

of [certain] diplomats”⁷⁵). 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 encryption⁷⁶, 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/29/32⁷⁷). Many commentators oppose state-attempts to compromise encryption.⁷⁸ 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.⁷⁹ The cited HRC resolution calls on states not to interfere with the use of encryption.⁸⁰ The Internet Society recommends the following⁸¹: “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.”⁸²

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.⁸³

⁷⁵ 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

⁷⁶ See for example <https://www.bloomberg.com/news/articles/2017-07-10/australia-s-turnbull-urges-internet-providers-to-block-extremism> and <https://www.diplomacy.edu/blog/2018predictions#9>

⁷⁷ <https://documents-dds-ny.un.org/doc/UNDOC/GEN/G15/095/85/PDF/G1509585.pdf?OpenElement>

⁷⁸ 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>

⁷⁹ See in particular pp. 54 ff. The Report is at: <http://unesdoc.unesco.org/images/0024/002465/246527e.pdf>

⁸⁰ See 9 of the cited HRC Resolution

⁸¹ 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>

⁸² Page 39 of the cited ISOC report.

⁸³ See for example p. 66 of GCI; and

<https://www.internetsociety.org/blog/2017/10/krack-reinforces-need-encryption-multiple-layers-stack/>

Secrecy of telecommunications is guaranteed by article 37 of the ITU Constitution. However, this provision appears to be out of date and to require modernization⁸⁴. In particular, restrictions must be placed on the collection and aggregation of meta-data.⁸⁵

There does not appear to be adequate consideration of the issues outlined above at the international level.⁸⁶

We recommend to invite IETF, ISOC, ITU, and OHCHR⁸⁷ to study the issues of privacy, encryption and prevention of inappropriate mass surveillance, which include technical, user education, and legal aspects.

3. 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 dominant⁸⁸. 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 effects⁸⁹, then a situation akin to a natural monopoly⁹⁰ might arise, there might be abuse of dominant market power⁹¹, and regulatory

⁸⁴ For a specific proposal, see the last page of the proposals at:

https://justnetcoalition.org/sites/default/files/HCHR_report_final.pdf

⁸⁵ See p. 31 of GCIg.

⁸⁶ See paragraph 46 of

http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session34/Documents/A_HRC_34_60_EN.docx

⁸⁷ 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> and

<http://www.ohchr.org/Documents/Issues/Privacy/DraftLegalInstrumentGovernmentLed.pdf>

⁸⁸ <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/>

⁸⁹ 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/>; see also

pages 9 and 12 of UNCTAD's *Information Economy Report 2017: Digitalization, Trade and Development*,

<http://unctad.org/en/pages/PublicationWebflyer.aspx?publicationid=1872>

⁹⁰ https://en.wikipedia.org/wiki/Natural_monopoly

⁹¹ <https://newint.org/features/2016/07/01/smiley-faced-monopolists/>; and the more radical criticism at:

http://www.rosalux-nyc.org/wp-content/files_mf/scholz_platformcoop_5.9.2016.pdf; specific criticism of a

dominant online retailer is at: <http://www.truth-out.org/news/item/38807-1-of-every-2-spent-online-goes-to-amazon-can-we-break-the-company-s-stranglehold> and <https://ilsr.org/amazon-stranglehold/>; see also:

http://www.nytimes.com/2016/12/13/opinion/forget-att-the-real-monopolies-are-google-and-facebook.html?_r=0; and:

<https://www.theguardian.com/commentisfree/2017/feb/19/the-observer-view-on-mark-zuckerberg>, and

<https://www.theatlantic.com/technology/archive/2018/01/facebook-doesnt-care/551684/>.

For a survey indicating that users are concerned about this issue, see:

https://ec.europa.eu/futurium/en/system/files/ged/ec_ngi_final_report_1.pdf.

For a very cogent historical analysis, making an analogy to the age of the Robber Barons, see:

intervention is required⁹². For example, platforms might abusively use personal data to set high prices for goods for certain customers,⁹³ or a dominant national provider might impede the operation of an international competitor⁹⁴, or a dominant company may excessively influence governments⁹⁵, or a dominant search engine might provide search results that favor certain retail sites⁹⁶. As the founders of Google put the matter back in 1998 (when they were graduate students): “we believe the issue of advertising causes enough mixed incentives that it is crucial to have a competitive search engine that is transparent and in the academic realm”⁹⁷.

Such corporate power can erode democracy, by in effect shifting power from the democratically elected representatives of the people to corporations, which not democratic entities. A scholarly article well documents the current trend towards shifting decision-making powers to private companies and concludes (the considerations below apply to many companies in addition to Amazon)⁹⁸:

Solutions to Amazon’s power will, no doubt, be hard to advance as a political matter—consumers like 2-day deliveries. But understanding the bigger picture here is a first step. Political economy clarifies the stakes of Amazon’s increasing power over commerce. We are not simply addressing dyadic transactions of individual consumers and merchants. Data access asymmetries will disadvantage each of them (and advantage Amazon as the middleman) for

<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>

⁹² 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> and

<https://www.economist.com/news/leaders/21735021-dominance-google-facebook-and-amazon-bad-consumers-and-competition-how-tame>; see also:

<https://www.nytimes.com/2017/04/22/opinion/sunday/is-it-time-to-break-up-google.html> ; and

<https://www.ip-watch.org/2017/05/09/republica-2017-strategy-empire-revealed-patents/> and

pp. 52 ff. of <http://www.autoritedelaconcurrence.fr/doc/reportcompetitionlawanddatafinal.pdf> and

<https://www.insidetechmedia.com/2017/11/07/the-bundeskartellamt-publishes-a-paper-on-big-data-and-competition/> .

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.

⁹³ <https://www.theguardian.com/technology/2017/jun/04/surge-pricing-comes-to-the-supermarket-dynamic-personal-data>

⁹⁴ <https://techcrunch.com/2016/11/28/ubers-china-app-is-now-separate-from-its-global-app-and-a-nightmare-for-foreigners/>

⁹⁵ 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>

⁹⁶ The European Commission found that Google had done this, see:

http://europa.eu/rapid/press-release_STATEMENT-17-1806_en.htm

http://europa.eu/rapid/press-release_MEMO-17-1785_en.htm

⁹⁷ At the end of Appendix A of the paper by Brin and Page, “The Anatomy of a Large-Scale Hypertextual Web Search Engine” at <http://infolab.stanford.edu/~backrub/google.html>

⁹⁸ <https://lpeblog.org/2017/12/06/from-territorial-to-functional-sovereignty-the-case-of-amazon/>

years to come. Nor can we consider that power imbalance in isolation from the way Amazon pits cities against one another. Mastery of political dynamics is just as important to the firm's success as any technical or business acumen. And only political organization can stop its functional sovereignties from further undermining the territorial governance at the heart of democracy.

As the Internet Society puts the matter on page 40 of its 2017 Global Internet Report: Paths to Our Future⁹⁹: “ ... 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 competition¹⁰⁰. As a learned commentator puts the matter¹⁰¹:

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.¹⁰² As one commentator puts the matter¹⁰³ (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.

⁹⁹ <https://future.internetsociety.org/wp-content/uploads/2017/09/2017-Internet-Society-Global-Internet-Report-Paths-to-Our-Digital-Future.pdf>

¹⁰⁰ <https://www.wired.com/story/ai-and-enormous-data-could-make-tech-giants-harder-to-topple/>

¹⁰¹ <https://www.theguardian.com/commentisfree/2016/dec/04/data-populists-must-seize-information-for-benefit-of-all-evgeny-morozov>

¹⁰² <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 .

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>

¹⁰³ 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>

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 matter¹⁰⁴:

... 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 a well-researched report put the matter: “[Company X’s] increasing dominance comes with high costs. It’s eroding opportunity and fueling inequality, and it’s concentrating power in ways that endanger competition, community life, and democracy. And yet these consequences have gone largely unnoticed thanks to [Company X’s] remarkable invisibility and the way its tentacles have quietly extended their reach.”¹⁰⁵

As noted above, the dominance of certain platforms¹⁰⁶ raises issues related to freedom of speech, because some platforms apply strict rules of their own to censor certain types of content¹⁰⁷, and, for

¹⁰⁴ 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>

¹⁰⁵ <https://ilsr.org/amazon-stranglehold/>

¹⁰⁶ For data regarding such dominance, see for example:

http://www.eecs.umich.edu/eecs/about/articles/2009/Observatory_Report.html

<http://www.networkworld.com/article/2251851/lan-wan/the-internet-has-shifted-under-our-feet.html>

<http://www.xconomy.com/boston/2009/10/20/arbor-networks-reports-on-the-rise-of-the-internet-hyper-giants/>

<https://www.arbornetworks.com/blog/asert/the-battle-of-the-hyper-giants-part-i-2/>

¹⁰⁷ See for example <https://www.theguardian.com/technology/2016/sep/09/facebook-deletes-norway-pms-post-napalm-girl-post-row>

many users, there are no real alternatives to dominant platforms¹⁰⁸; and some workers might also face limited choices due to dominant platforms¹⁰⁹.

As *The Economist* puts the matter¹¹⁰:

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.¹¹¹

And, citing *The Economist* again¹¹²:

The dearth of data markets will also make it more difficult to solve knotty policy problems. Three stand out: antitrust, privacy and social equality. The most pressing one, arguably, is antitrust ...

As learned scholars have put the matter¹¹³:

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.

¹⁰⁸ <https://www.theguardian.com/technology/2016/nov/17/google-suspends-customer-accounts-for-reselling-pixel-phones>

¹⁰⁹ https://www.nytimes.com/2017/03/21/magazine/platform-companies-are-becoming-more-powerful-but-what-exactly-do-they-want.html?_r=2

¹¹⁰ <http://www.economist.com/news/leaders/21707210-rise-corporate-colossus-threatens-both-competition-and-legitimacy-business>

¹¹¹ <https://disruptive.asia/transit-dead-content-literally-rules/>

¹¹² <http://www.economist.com/news/briefing/21721634-how-it-shaping-up-data-giving-rise-new-economy>

¹¹³ 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>

An excellent overview of various methods that can be used to increase competition is provided in Wu, Tim, Antitrust Via Rulemaking: Competition Catalysts (October 24, 2017), *Colorado Technology Law Journal*.¹¹⁴ Wu refers to actual examples (including in telecommunications) to show how regulations can be used to increase (or inadvertently fail to increase) competition. That is, regulatory intervention is means to be considered in parallel to, or instead of, judicial enforcement of antitrust/competition law.

Measures to ensure accountability may be needed with respect to labor-relation issues, and not only with respect to users and consumers.¹¹⁵

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.”¹¹⁶

National authorities in a number of countries have undertaken investigations,¹¹⁷ and even imposed measures,¹¹⁸ 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.”¹¹⁹ The Legal Affairs Committee of the European Parliament adopted an Opinion in May 2017 that, among other provisions¹²⁰:

Calls for an appropriate and proportionate regulatory framework that would guarantee responsibility, fairness, trust and transparency in platforms’ processes in order to avoid discrimination and arbitrariness towards business partners, consumers, users and workers in relation to, inter alia, access to the service, appropriate and fair referencing, search results, or the functioning of relevant application programming interfaces, on the basis of interoperability and compliance principles applicable to platforms;

The topic is covered to some extent in paragraphs 24 ff. of a European Parliament Committee Report on online platforms and the digital single market, (2016/2276(INI)).¹²¹ And by some provisions in the

¹¹⁴ <https://ssrn.com/abstract=3058114>

¹¹⁵ https://www.nytimes.com/interactive/2017/04/02/technology/uber-drivers-psychological-tricks.html?_r=2

¹¹⁶ <https://www.theguardian.com/commentisfree/2016/dec/04/data-populists-must-seize-information-for-benefit-of-all-evgeny-morozov>

¹¹⁷ 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>

¹¹⁸ See for example http://www.autoritedelaconcurrence.fr/user/standard.php?id_rub=606&id_article=2534

and, in the case of Google: http://europa.eu/rapid/press-release_IP-17-1784_en.htm

¹¹⁹ <http://www.cnet.com/news/senator-warren-says-apple-google-and-amazon-have-too-much-power/>

¹²⁰ <http://www.europarl.europa.eu/sides/getDoc.do?type=COMPARL&reference=PE-601.100&format=PDF&language=EN&secondRef=02>

¹²¹ <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+COMPARL+PE-599.814+01+DOC+PDF+V0//EN&language=EN>

national laws of at least one country.¹²² Many of the issues relating to platforms and human rights have been well documented by the IGF Dynamic Coalition on Platform Responsibility.¹²³

However, it does not appear that there is an adequate platform for exchanging national experiences regarding such matters.¹²⁴

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.¹²⁵

We recommend to invite UNCTAD to study the economic and market issues related to platform dominance¹²⁶, 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.¹²⁷

¹²² See section 3.2 of the following commentary on the French Digital Republic Law:

<https://www.lw.com/thoughtLeadership/French-digital-republic-law-english> ;

see also the decrees issued in October 2017:

<http://proxy-pubminefi.diffusion.finances.gouv.fr/pub/document/18/22764.pdf>

¹²³ <http://bibliotecadigital.fgv.br/dspace/handle/10438/19402>

¹²⁴ 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>

¹²⁵ 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>

¹²⁶ 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>

¹²⁷ <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> and

the comments starting at 13 minutes, 30 seconds, in the excellent talk at:

https://www.ted.com/talks/zeynep_tufekci_we_re_building_a_dystopia_just_to_make_people_click_on_ads/ ;

for a possible impact on free speech, see:

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

We recommend to invite UN HCHR to study the potential effects of platform dominance on elections and democracy.

4. Privacy and data protection must not be negotiated as free trade issues

Discussions that are planned to take place in the context of the World Trade Organization (WTO) could have significant implications for data privacy¹²⁸. As two experts put the matter¹²⁹:

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

...

Never before has a trade negotiation had such a limited number of beneficiaries. Make no mistake, what will be discussed there, with the South arriving unprepared, will affect each and every space, from government to health, from development to innovation going well beyond just trade. Data is the new oil – and we need to start organising ourselves for the fourth industrial revolution. The data lords, those who have the computational power to develop superior products and services from machine learning and artificial intelligence, want to make sure that no domestic regulation, no competition laws, privacy or consumer protection would interfere with their plans.

...

Disguised as support for access and affordability, they [dominant Internet data-driven companies] want everyone to connect as fast as they can. Pretending to offer opportunities to grow, they want to deploy and concentrate their platforms, systems and content everywhere in the world. Enforcement measures will be coded in technology, borders for data extraction will be blurred, the ability to regulate and protect the data of citizens will be disputed by

¹²⁸ See for example WTO documents JOB/SERV/248/Rev.2 and TN/S/W/64. See in this context our submission to the ITU Council Working Group on Internet-related Public Policy Issues, at:

<http://www.itu.int/en/council/cwg-internet/Pages/display-June2017.aspx?ListItemID=5> .

For an overall analysis of the WTO proposals, see:

http://www.huffingtonpost.com/entry/state-of-play-in-the-wto-toward-the-11th-ministerial_us_5951365ae4b0f078efd98399 ; see also:

<http://www.itu.int/en/council/cwg-internet/Pages/display-June2017.aspx?ListItemID=7> and

<https://www.diplomacy.edu/blog/2018predictions#3>

¹²⁹ <https://www.opendemocracy.net/digitaliberties/renata-avila-burcu-kilic/new-digital-trade-agenda-are-we-giving-away-internet>

supranational courts, as local industries cannot compete and local jobs soar. If we are not vigilant, we will rapidly consolidate this digital colonisation, a neo-feudal regime where all the rules are dictated by the technology giants, to be obeyed by the rest of us.

Criticism of holding discussions related to the Internet in the WTO and other trade negotiation forums is not all that recent. Pages 74-75 of UNCTAD's *Information Economy Report 2017: Digitalization, Trade and Development*¹³⁰ contain the following citations:

“Bilateral and multilateral free trade agreements can significantly affect Internet governance issues. Many, such as the Trans-Pacific Partnership Agreement, specifically address important issues such as data localization, encryption, censorship and transparency, all of which are generally regarded as forming part of the Internet governance landscape. However, they are negotiated exclusively by governments and usually in secret. At the same time, such agreements substantially benefit the Internet in a myriad of ways, such as by agreeing on rules to improve competition and market access. Further agreements such as the US-Europe Transatlantic Trade and Investment Partnership and the Trade in Services Agreement under the World Trade Organization are expected to cover similar territory. The fact that these negotiations are open only to governments has inspired protests by non-governmental actors demanding that they be informed and engaged in negotiations to allay fears that the new rules embedded in these agreements favour the interests of governments or corporations over those of other Internet users. The closed nature of the negotiations also means that the benefits governments hope to achieve may not be evident to the general public (GCIIG, 2016: 78).”¹³¹

and

“We recognize the considerable social and economic benefits that could flow from an international trading system that is fair, sustainable, democratic, and accountable. These goals can only be achieved through processes that ensure effective public participation. Modern trade agreements are negotiated in closed, opaque and unaccountable fora that lack democratic safeguards and are vulnerable to undue influence. These are not simply issues of principle; the secrecy prevents negotiators from having access to all points of view and excludes many stakeholders with demonstrable expertise that would be valuable to the negotiators. This is particularly notable in relation to issues that have impacts on the online and digital environment, which have been increasingly subsumed into trade agreements over the past two decades.”¹³²

¹³⁰ <http://unctad.org/en/pages/PublicationWebflyer.aspx?publicationid=1872>

¹³¹ The source is the report of the Global Commission on Internet Governance, at: http://ourinternet.org/sites/default/files/inline-files/GCIIG_Final%20Report%20-%20USB.pdf.

¹³² The source is the Open Digital Trade Network Brussels Declaration, at: https://www.eff.org/files/2016/03/15/brussels_declaration.pdf

The cited UNCTAD report goes on to state:

“Stakeholders have also expressed concerns about various substantive aspects of rules governing trade in the digital economy. Contentious issues include the inclusion of provisions concerning intellectual property, encryption, source codes, intermediary liability, network neutrality, spam, authentication and consumer protection.”¹³³

As one academic analysis puts the matter: “The new e-commerce regime is not about ‘free trade’ and barely about real commerce. As with the WTO’s Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS), it aims to protect and entrench the oligopoly of first movers”.¹³⁴ The dangers of viewing data as a commodity that should flow freely are well explained in a paper by IT for Change.¹³⁵ As two experts put the matter¹³⁶:

But if all the world’s data flows back to a few tech powerhouses, without restrictions or taxes, this will further reinforce their monopolies, widen the privacy gap, and leave developing countries as passive consumers or data points, rather than participants in the digital economy.

Those calling for liberalization use the rhetoric of creating opportunities for the poor — connecting the next billion — which sounds great, but only if we disconnect it from reality. Today, 60% world lacks even access to electricity. In the past, Spanish colonizers arrived in the Americas offering mirrors to the indigenous people in exchange for their gold. Is connectivity the “mirror” powerful actors are offering to the global poor today?

Trade agreements eliminate the diversity of domestic policies and priorities, and impose costly restrictions on countries that want to address local inequalities and boost local industry. In the case of the digital economy, it will consolidate the position of few, to the detriment of the rest.

The scope of the provisions proposed in free trade negotiations is very broad and goes well beyond what the traditional scope of WTO.¹³⁷ And, as the cited scholar¹³⁸ puts the matter, citing other scholars: “We find ourselves in ‘ . . . a system that officially claims to embrace free trade, yet still pits one political interest against another in a quest to seize protectionist rents. Powerful lobbies, such as domestic

¹³³ The cited UNCTAD report gives the following source for that statement: “Bureau Européen des Unions de Consommateurs (BEUC), Analysis of the TiSA e-commerce annex & recommendations to the negotiators, TiSA leaks, September 2016 (http://www.beuc.eu/publications/beuc-x-2016-083_lau_beucs_analysis_e-commerce_tisa_2016.pdf , accessed 1 June 2017); and EDRI’s red lines on TTIP, January 2015 (https://edri.org/files/TTIP_redlines_20150112.pdf , accessed 1 June 2017). BEUC and EDRI are coalitions of 43 and 35 civil society organizations, respectively.”

¹³⁴ Page 2 of Kelsey, Jane (2017) *The Risks for ASEAN of New Mega-Agreements that Promote the Wrong Model of e-Commerce*, ERIA Discussion Paper 2017-10, available at: http://www.eria.org/publications/discussion_papers/DP2017-10.html

¹³⁵ <http://www.itforchange.net/sites/default/files/add/The%20grand%20myth%20of%20cross-border%20data%20flows%20in%20trade%20deals-Dec2017.pdf>

¹³⁶ <https://www.buzzfeed.com/burcukilic/big-tech-is-pushing-for-a-new-kind-of-free-trade>

¹³⁷ See for example pp. 101 ff. of the academic analysis at:

https://lawreview.law.ucdavis.edu/issues/51/1/Symposium/51-1_Burri.pdf

¹³⁸ *Op. cit.*, p. 129

producers, capture trade negotiators and replace national interests with those of their own.”
Negotiations in trade venues proceed “in a secretive, non-transparent, and non-inclusive manner.”¹³⁹

In light of the fundamental importance of transparency and inclusiveness in discussions of data privacy and data protection, we recommend inviting governments to refrain from discussing those matters in forums that are not transparent or inclusive. In particular we recommend inviting governments not to discuss in the context of the WTO or plurilateral forums such as the Trade in Services Agreements (TISA) matters such as the free flow of. We recommend to invite governments to discuss matters related to the free flow of data only in forums that are transparent and inclusive, and in accordance with the roles and responsibilities outlined in paragraph 35 of the Tunis Agenda.

¹³⁹ *Op. cit.*, p. 130