Trade War, Big Data and Algorithms

Dr. Kung-Chung LIU*/Jianchen LIU**

Abstract

The breakout of the trade war between the US and China seems inevitable for at least three reasons: (1) both countries have entered the era of the data-driven economy, and yet most of the biggest data collectors and exploiters of the world (e.g. Google and Facebook) headquartered in the US are shut out of China, (2) the world trading order under the WTO is pre-Internet and therefore the Internet suffers from a vacuum of global order and governance, and (3) China's ideological leaning is extremely different, and this is magnified by its leadership's ambitious outreach initiatives. A new world trade order under a functional global governance is needed, which can only be established if the US and China can settle on (1) the rules for the exploitation of big data (cross-border flow of big data, data mining etc.), and (2) how to audit algorithms that decide the collection and use of big data.

1. Trade war

1.1. Bound to happen

To some, the US-China trade war might come as a surprise. However, it was bound to happen in the era of the data-driven economy for the following reasons:

Firstly, major US tech giants, Google, Facebook, Twitter etc., which are without exception the biggest data collectors, generators and exploiters of the world, were driven out of or banned in China.[1] Google shut down its Chinese operations in 2010, allegedly after it discovered a cyberattack from within China that targeted it and dozens of other companies.[2] Foreign news media, also big data collectors, generators and exploiters, are highly restricted in China too. A foreign media organization that intends to establish an office in China or dispatch a resident journalist to China needs the

*Lee Kong Chian Professor of Law (Practice), Director, Applied Research Centre for Intellectual Assets and the Law in Asia (ARCIALA), School of Law, Singapore Management University/Renmin University of China. This research is supported by the National Research Foundation, Prime Minister's Office, Singapore under its Emerging Area Research Project Funding Initiative.**Research Associate, ARCIALA, PhD candidate at Renmin University of China; his contribution is partly supported by the Fundamental Research Funds for the Central Universities and the Research Funds of Renmin University of China (19XNH018). All online materials have been accessed before July 2019.

[1] While China blocked Facebook and Twitter, Google has voluntarily pulled out of China. See International Business Times: China Defends Blocking Facebook, Twitter and Bloomberg, https://www.ibtimes.co.uk/china-defends-blocking-facebook-twitter-bloomberg-1432488

[2] The Atlantic, Why Google Quit China—and Why It's Heading Back, https://www.theatlantic.com/technology/archive/2016/01/why-google-quit-china-and-why-its-heading-back/424482/. It has been reported in 2018 that Google was heading back to China with a project named "Project Dragonfly" that would censor certain terms and news outlets to comply with China's laws; however, this was shut down due to violation of Google's core values. See TECHSPOT: Google has reportedly shut down its 'Dragonfly' Chinese search engine project, https://www.techspot.com/news/77909-google-has-reportedly-shut-down-dragonfly-chinese-search.html

approval of the Foreign Ministry.[3] Foreign press needs permission to publish anything online in China. A substantial amount of foreign websites, including non-US ones such as the BBC and Deutsche Welle, are blocked in China.[4] In stark contrast, China has set up a host of printing and electronic news media worldwide without encountering legal hurdles.[5]

On a related front, China has initiated a series of antitrust investigations against multinational companies, and the number is on the rise since 2013. For example, InterDigital, Qualcomm and Tetra Pak were investigated in 2013, Microsoft in 2014, Mercedes Benz in 2015, Medtronic in 2016, and DowDuPont, Micron, Samsung Electronics, and SK Hynix in 2017.[6] As a result, Qualcomm was imposed a heavy fine of RMB 6 billion (≈US$ $975 million) and ordered to stop abusing its dominant market position, such as charging royalties for expired patents, bundling standard essential patents (SEPs) with non-SEPs, and forcing licensees to offer free grant-back license of their patents. In addition to offering to the authority to revise its licensing practice, Qualcomm even "agreed" not to appeal.[7] The feeling by American enterprises of being treated unequally in China by the Chinese government is staggering.

Secondly, China has been accused by the US of cheating on the world trade order represented by the World Trade Organisation (WTO) and building market access barriers. In one prominent example, in the Protocol on the Accession of the People's Republic of China (Accession Protocol), China has committed to opening up the telecommunication market to foreign operators, and yet no meaningful market opening has taken place thus far.[8] According to Thomas Friedman, one of the three pillars supporting China's economic success is that China has a system of cheating on WTO rules, including forced transfers of technology, the stealing of the intellectual property (IP) of others, nonreciprocal trade rules, and massive government support for the winners of both its Darwinian

[3] Article 6 of the Regulations of the People's Republic of China on News Coverage by Permanent Offices of Foreign Media Organizations and Foreign Journalists.

[4] See Newsweek: China Set to Block All Foreign Media from Publishing without Permission, https://www.newsweek.com/china-ban-foreign-media-online-428550.

[5] According to World Economic Forum, Xinhua News Agency currently has over 180 news bureaus globally; China Central Television has over 70 foreign bureaus, broadcasting to 171 countries and regions in six UN official languages; China Radio International, the world's second biggest radio station next to the BBC, broadcasts in 64 languages from 32 foreign bureaus, reaching 90 radio stations worldwide; other official Chinese media including China Daily, People's Daily, and Economic Daily are all stepping up efforts in going global. See Vivian Yang, How Chinese media is going global, https://www.weforum.org/agenda/2015/08/how-chinese-media-is-going-global/

[6]Cited from a statistical table by Todd Liao & Bonnie Li: Antitrust Dawn Raids in China: On the Tenth Anniversary of Chinese Antitrust Enforcement, China Antitrust Law Journal, Vol. 10, 2018, pp. 3-4.

[7] See Administrative Decision of the National Development and Reform Commission of China (2015) No. 1.

[8] China has committed to permitting foreign operators to provide a broad range of telecommunications services through joint ventures with Chinese companies. See China's Accession Protocol, pp. 16-17. However, with regard to basic services, the Ministry of Industry and Information Technology of China (MIIT) has imposed informal bans on new entry, limitations on foreign operators' selection of Chinese joint venture partners, and high capital requirements, which has presented formidable barriers to market entry for foreign suppliers. In addition, the approach that China has taken to regulate value-added services, including its insistence on classifying certain value-added services as basic services when provided by foreign operators, amounts to similarly formidable barriers to foreign entry. See USTR, 2018 Report to Congress on China's WTO Compliance (February 2019), p. 154, available at: https://ustr.gov/sites/default/files/2018-USTR-Report-to-Congress-on-China%27s-WTO-Compliance.pdf

competitions and inefficient state-owned industries.[9] Furthermore, the world trading order under the WTO was built in 1994, prior to the advent of the Internet. Therefore, there has clearly been a vacuum of global governance on the Internet, not to mention big data and algorithms.

Thirdly, the traditional telecommunication networks and the Internet are the infrastructure for the generation, transmission, and collection of data. For a level playing field for parties involved in the rollout and operation of telecom and the Internet, domestic and foreign alike, it is imperative to have in place a law on telecommunications and the Internet. However, China has only an administrative regulation promulgated by the State Council in 2000. The long-promised Telecommunications Law has not been enacted to date.[10]

The final, possibly the ultimate, and yet unspoken reason triggering the trade war is the revocation of the two-term limitation for the president of China in 2017, which has crossed the red line of the West,[11] coupled with the Chinese government's large-scale outreach initiatives, such as One Belt One Road (B&R).[12]

1.2. Flanked and even carried further by legal battles

The US is taking a two-prong approach to legally flank and even escalate its trade war with China. On the one hand, rather than building the WTO further to fill the regulatory vacuum, the US is weakening or even dismantling the WTO multilateralism by discrediting and attacking it,[13] paralyzing its Appellate Body (AB), composed of seven members with four-year term and a quorum of three, through delaying the appointment of AB's members.[14] There are currently three members in the AB,

[9] Thomas Friedman, China and Trump, Listen Up!, https://www.nytimes.com/2018/11/13/opinion/china-trump-trade.html

[10] MIIT prepared a draft Telecommunications Law in July 2004 and submitted it to the State Council for review. MIIT has further revised the draft based on the State Council's feedback and will again solicit public opinion once it is ready. See MIIT, A Reply to No. 3129 Suggestion by a representative of the National People's Congress, dated 5 July 2017, available at: http://www.miit.gov.cn/n1146295/n1146592/n3917132/n4545264/c5737165/content.html

[11] See US-China Perception Monitor, The World Reacts to China's Constitutional Amendment, https://www.uscnpm.org/blog/2018/03/19/world-reacts-chinas-constitutional-amendment/

[12] The B&R, when seen through the lens of the Singapore government (https://ie.enterprisesg.gov.sg/venture-overseas/browse-by-market/asia-pacific/china/about-obor), "is the Chinese government's development strategy to build ties along the overland Silk Road Economic Belt and the naval trading route known as the 21st Century Maritime Silk Road. Through infrastructural development, it aims to promote the flow of people, goods, capital and ideas between Asia, Africa and Europe. The initiative was introduced by China President Xi Jinping in 2013, with the aim of connecting about 80 countries across three continents to China."

[13] See Anwarul Hoda, Collapsing Trade Order: How the WTO is under Attack, https://www.financialexpress.com/opinion/collapsing-trade-order-how-the-wto-is-under-attack/1361601/

[14] Candidates for the AB have come under increasingly close scrutiny—and frequently are blocked if their previous writings appear problematic to the US. This means that most international court judges face the prospect of having their reappointments blocked, either by the states that nominated them (typically their home state) or by other states. The U.S. in 2011 denied a second term in the AB to Jennifer Hillman, a widely respected U.S. member of the AB, raising early concerns about the AB's judicial independence. Besides, it also opposed a second term for Seung Wha Chang from South Korea in 2016, which is considered an escalation because for the first time it involves the reappointment of a non-U.S. judge. Each member of the AB may be reappointed for another four years, and such reappointment is almost automatic. Denial of reappointment for a second term was clearly aimed at curtailing the independence of AB members. Most recently, the US on Sep. 26, 2018 again blocked the launch of the selection processes to fill four vacancies. See Manfred Elsig, Mark

and only one will remain by December 2019. By then, the AB will cease to function.[15] The US even threatens to leave the WTO.[16]

On the other hand, the US is using the "market economy" status in the anti-dumping context as a lever to isolate China if needed. Article 15(a)(ii) of the Accession Protocol is about how to assess the price for comparison for China's industries to determine the dumping margin, and allows 'The importing WTO Member … [to] use a methodology that is not based on a strict comparison with domestic prices or costs in China if the producers under investigation cannot clearly show that market economy conditions prevail in the industry producing the like product with regard to manufacture, production and sale of that product.' Article 15(d) of the Accession Protocol continues to mandate that 'In any event, the provisions of subparagraph (a)(ii) shall expire 15 years after the date of accession.' This is one of the three ways to cease applying Article 15(a)(ii). In December 2016 China asserted that it has been a member of the WTO for 15 years, therefore Article 15(a)(ii) should cease to apply in two antidumping cases. Yet the US and the EU insisted on keeping the old methodology. The US and the EU are of the opinion that 'the legal authority to reject prices or costs not determined under market economy conditions' flows from anti-dumping clause of Article VI(1) and (2) of the General Agreement on Tariffs and Trade (GATT) 1994 and the need to ensure comparability of prices and costs, and that the expiry of the 15-year period simply shifts the burden of proof.[17] According to the US and the EU, before the expiry, it was the producers who had to prove market economy conditions; after the expiry, members of the WTO can still reject domestic prices if they can prove the nonexistence of market economy conditions.[18]

China's remaining a non-market economy could have other grave ramifications for China. For one thing, the US can further block its trading partners from signing free trade agreements (FTAs) with China. One concrete example is the United States–Mexico–Canada Agreement (USMCA). Article 32.10 (4) of USMCA provides: 'Entry by a Party into a free trade agreement with a non-market

---

Pollack and Gregory Shaffer, The U.S. is causing a major controversy in the World Trade Organization, available at https://www.washingtonpost.com/news/monkey-cage/wp/2016/06/06/the-u-s-is-trying-to-block-the-reappointment-of-a-wto-judge-here-are-3-things-to-know/?utm_term=.492d2eeecbb5; see also Third World Network, US continues to stymie WTO efforts over AB appointments, https://twn.my/title2/wto.info/2018/ti181005.htm

[15] See Article 17 of the Dispute Settlement Understanding; see also WTO: Appellate Body Members, https://www.wto.org/english/tratop_e/dispu_e/ab_members_descrp_e.htm.

[16] On many occasions President Donald Trump threatens to pull US out of the WTO if it fails to shape up, https://www.theblaze.com/news/2018/08/31/trump-threatens-to-pull-us-out-of-the-world-trade-organization-if-it-fails-to-shape-up

[17] Such a "Shifting the Burden of Proof" approach was advocated by Jorge Miranda, then adopted by the EU and the US. See Jorge Miranda, "Interpreting Paragraph 15 of China's Protocol of Accession" (2014)9(3) Global Trade and Customs Journal, pp. 94-103; Jorge Miranda, "More on Why Granting China Market Economy Status after December 2016 Is Contingent upon Whether China Has in Fact Transitioned into a Market Economy"; Jorge Miranda, "Implementation of the 'Shift in Burden of Proof' Approach to Interpreting Paragraph 15 of China's Protocol of Accession" (2016)11(10) Global Trade and Customs Journal, pp. 447-453.

[18] See European Union – Measures Related to Price Comparison Methodologies (DS516), First Written Submission by the European Union (EU Submission), Nov. 14, 2017, paras. 95-118, available at: http://trade.ec.europa.eu/doclib/docs/2017/november/tradoc_156401.pdf; Office of the USTR, European Union – Measures Related to Price Comparison Methodologies, Legal Interpretation – GATT 1994 Article VI:1; Second Note Ad Article VI:1; Practice of GATT Contracting Parties; Accessions to GATT; ADA Article 2; and Section 15 China WTO Accession Protocol (US Interpretation), Nov. 13, 2017, paras. 8.1-8.5.6, available at: https://ustr.gov/sites/default/files/enforcement/WTO/US.Legal.Interp.Doc.fin.%28public%29.pdf

country will allow the other Parties to terminate this Agreement on six months' notice and replace this Agreement with an agreement as between them.'[19] According to Article 32.10(1) thereof, a non-market country is a country: '(a) that on the date of signature of this Agreement, a Party has determined to be a non-market economy for purposes of its trade remedy laws; and (b) with which no Party has signed a free trade agreement.'[20] Since the U.S. deems China a non-market economy, Mexico and Canada would not take the risk of signing an FTA with China, leaving China no chance to be a free trade partner with any of them. In addition, on September 28, 2018 trade ministers from Japan, the EU and the US have agreed on specific measures to address third countries' unfair trade behavior, which refers to (a) non-market-oriented policies and practices, (b) industrial subsidies and state-owned enterprises, and (c) forced technology transfer policies and practices, targeting China as a "third country."[21]

1.3. How will it unfold?

The US-China trade war has led to hiking of tariffs,[22] sanctions on individual Chinese companies (e.g. the US banned Huawei and ZTE equipment from being used by federal agencies and recipients of federal funding),[23] and their rejection by US allies (e.g. Australia, New Zealand and Japan have already effectively excluded Huawei from their 5G rollouts. Canada is considering following suit).[24] The entire exclusion of one specific Chinese industry, such as 5G equipment, is one possible next punishment. There is no legal remedy available for the Chinese government and companies, as, internationally, the dispute settlement body of the WTO will cease to function by December 2019, and, domestically, there is no judicial review of the exercise of the presidential executive power in

[19] See Article 32.10 (4) of the USMCA.

[20] See Article 32.10 (1) of the USMCA.

[21] Mizuho Research Institute, Mizuho Economic Outlook & Analysis—Japan's trade policy challenges in 2019, p. 5, available at: https://www.mizuho-ri.co.jp/publication/research/pdf/eo/MEA190206.pdf

[22] In the first round of the US-China trade war, the US hiked the import tariff to 25% on US$50 billion worth of Chinese goods from July 6 to August 23, 2018. China, as a retaliatory measure, imposed tariffs of 25% on the same dollar amount of American products. In the second round, the US has imposed tariffs of 10% on US$200 billion worth of goods from China since September 24, 2018 and once threatened to raise this to 25% starting from January 1, 2019, while China imposed tariffs of up to 10% on another US$60 billion worth of American products. After a meeting between President Trump and President Xi Jinping at the G-20 summit on Dec. 1, 2018, tariffs on US$200 billion worth of goods from China will remain at the rate of 10% and not rise to 25%. However, the two administrations did not reach an agreement on the matters before March 1, 2019, and tariffs rose to 25%. See relevant press releases made by Office of the USTR, https://ustr.gov/about-us/policy-offices/press-office/press-releases/2018; see also Announcement of Tariff Commission of the State Council of China 2018 Nos. 5-8.

[23] ZTE was fined by the US government a record-high penalty of $1.19 billion for violating US sanctions against both Iran and North Korea by selling products to the two countries. See https://www.commerce.gov/news/press-releases/2017/03/secretary-commerce-wilbur-l-ross-jr-announces-119-billion-penalty. Huawei and its CFO Wanzhou Meng were charged by US federal investigators with financial fraud to sidestep US sanctions on Iran. See https://www.justice.gov/opa/pr/chinese-telecommunications-conglomerate-huawei-and-huawei-cfo-wanzhou-meng-charged-financial,

[24] However, Thailand has bucked the trend by launching a test of Huawei's 5G equipment. German media reports that its government is also not keen to implement a full ban. See Fortune, Trump Tipped to Ban Chinese Equipment from U.S. Mobile Networks, http://fortune.com/2019/02/08/trump-chinese-ban-5g.

trade.[25] In a sense, the Chinese government and companies are forced to relive Qualcomm's agony of having no legal relief.

2. Big data

The true cure for the trade war between the US and China lies not in the avoidance of the Thucydides trap, but solving problems related to big data[26] and algorithms. In the data-driven economy, big data, generated and collected by netizens and machines (devices) connected via the Internet of things (IoT), is like the crude oil or electricity for the development of new products or services, business models and artificial intelligence (AI). Big data analytics can help with profiling customers and increasing customer experiences, satisfaction and loyalty[27]. More importantly, according to Kai-Fu Lee, successful AI algorithms need three things, big data, computing power, and the work of strong—but not necessarily elite— AI algorithm engineers, and in this age of AI implementation, data is the key and China is the "Saudi Arabia of data."[28] Lee assesses that China is in a strong position to lead or co-lead in Internet AI and perception AI, and will likely soon catch up with the US in autonomous AI, while the US is clearly leading only in business AI. He predicts that by 2023 China will lead the US by a ratio of 6 to 4 and 8 to 2 in Internet AI and perception AI, and the US will lead China by 7 to 3 in business AI, while China and the US will tie in autonomous AI.[29]

2.1. The legal nature of big data

Heated debates about whether and how the current legal framework should respond or be adapted to solving problems raised by the special attributes of big data have been unleashed. The one with paramount importance is about the legal nature of big data, whether and how to protect it, and who, if anyone, "owns" it? There are several ways under discussion for "protecting" big data, such as

[25] For example, Section 301 of the US Trade Act of 1974 vests the US President with unbridled power to deal with unfair trade practices by foreign countries through investigation into their trade practices and taking counter-measures in response, including hiking import tariffs.

[26] This article defines big data as not including personal data, which is a separate issue mainly governed by privacy law. See, e.g., Paul Schwartz & Daniel Solove, The PII Problem: Privacy and a New Concept of Personally Identifiable Information, 86 N.Y.U.L. Rev. 1814 (2011); Robert Sloan & Richard Warner, Beyond Notice and Choice: Privacy, Norms, and Consent, 14 J. High Tech. L. 370 (2014); Jack Balkin, Information Fiduciaries and the First Amendment, 49 U.C. Davis L. Rev. 1183(2016).

[27] See Laika Satish & Norazah Yusof, A Review: Big Data Analytics for enhanced Customer Experiences with Crowd Sourcing, 116 Procedia Computer Science 274 (2017); Seshadri Tirunillai & Gerard J. Tellis, Extracting Dimensions of Consumer Satisfaction with Quality from Online Chatter: Strategic Brand Analysis of Big Data Using Latent Dirichlet Allocation (20 March 2014), available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2408855.

[28] Kai-Fu Lee, AI Superpowers— China, Silicon Valley and the New World Order, 2018, p. 14 and p. 55.

[29] Kai-Fu Lee, AI Superpowers— China, Silicon Valley and the New World Order, 2018, p. 106 and p. 136.

its propertization (exclusive right to use)[30] via IP rights (IPR), trade secret mechanism,[31] or sui generis protection. However, a "proprietary" approach is ill-suited for big data and the goal of the data-driven economy, namely to promote innovation, competition, economic growth and ultimately consumer welfare through generating, collecting and exploiting data at the speed of lightening. Admittedly, any exclusive right on big data will only slow down such speed. In addition, this approach suffers from the inability to determine the subject matter and the scope of protection, because the amorphous boundary of big data defies the characterization of property. In specific, granting an exclusive IPR lacks economic justification. Legal economists generally believe that IP law functions as a tool to cure market failure deriving from the "public goods" characteristics.[32] Public goods, once produced, are virtually inexhaustible, i.e. the use of specific data through one person would not prevent others from using the same, and its owners cannot prevent those who do not pay from using it.[33] Since it is difficult or expensive to prevent "free riders" from using public goods, IP law grants creators an exclusive right to forbid unauthorized use, and thus keeps them incentivized. However, big data does not fall under the category of public goods, as generally data holders are capable of excluding others from accessing and using their data.[34] Such control makes it almost impossible for others to get access to big data without data controllers' consent or license. For this reason, the current data industry does not lack incentives to collect, process, analyze and exploit

[30] On January 10, 2017, the EU Commission in its Communication "Building a European data economy" briefly discussed, among other things, the possibilities of granting data producers a new exclusive property right on data for non-personal (or anonymised) machine-generated data, which is named data producers' right, allowing them to use and authorise the use of such data. However, relevant exceptions would need to be clearly specified. See European Commission, Building a European Data Economy, COM (2017) 9 final, p. 13; European Commission, Staff Working Document to the Communication "Building a European data economy", SWD (2017) 2 final, pp. 33-36.

[31] Big data satisfying the requirements for trade secret, typically including secrecy, economic value and reasonable measures taken by data controllers to keep confidentiality, can enjoy trade secret protection. However, the majority of big data fall outside the scope of such protection. See Max Planck Institute for Innovation and Competition, Position Statement on Data Ownership and Access to Data, paras. 9-28, available at: http://www.ip.mpg.de/fileadmin/ipmpg/content/stellungnahmen/positionspaper-data-eng-2016_08_16-def.pdf. Therefore, the suggestion by Herbert Zech (A Legal Framework for a Data Economy in the European Digital Single Market: Rights to Use Data, Journal of Intellectual Property Law & Practice, 2016, p. 11) that granting a new IPR on data could help to disclose data that have been kept secret, to create markets for trading data, and leading to optimal allocation of data, is largely flawed.

[32] See Stan J. Liebowitz, Copyright and Photocopying: Alternative Institutional Arrangements 3-5 (Feb. 1981). Quoted from Wendy J. Gordon, Fair Use as Market Failure: A Structural and Economic Analysis of the Betamax Case and its Predecessors, 82 Colum. L. Rev. 1600, p. 1610 (1982). See also Frank P. Darr, Testing an Economic Theory of Copyright: Historical Materials and Fair Use, 32 B.C. L. REV. 1027, pp. 1033-1034 (1991).

[33] See, e.g., Daniel Orr, Property, Markets, and Government Intervention: A Textbook in Microeconomic Theory and Its Current Applications, Goodyear Publishing Co., Inc. (1976), pp. 285-311.

[34] As pointed out by Wolfgang Kerber, although there might be different kinds of data and therefore also the costs and the difficulty of keeping them secret might vary, generally data holders are capable of excluding others from copying and using their data. Such excludability, however, is an empirical question and might be subject to technical progress. See Wolfgang Kerber, A New (Intellectual) Property Right for Non-Personal Data? An Economic Analysis (October 24, 2016), Gewerblicher Rechtsschutz und Urheberrecht, Internationaler Teil (GRUR Int), 11/2016, 989-999, pp. 9-10, available at SSRN: https://ssrn.com/abstract=2858171.

data. It is therefore safe to say the market still functions, and thus there is no identifiable market failure existing.[35]

It is only fair to think that we, the netizens (including institutions which install devices that generate data), not any individual companies, are the creators and "owners" of big data. However, internet companies, through which netizens and devices are interconnected with one another, have de facto control over big data, and may "sell" or "license" others to use it, without having legal ownership of exclusive property over big data according to the prevailing view in academia.[36]

2.2. Access to and trading of big data

It is easily conceivable that if companies in the industry all have access to big data, more and better products and services would be provided to consumers. The thriving e-commerce via APPs on the smart phones in China is one compelling example. Especially when big data cannot be reproduced or otherwise obtained, access to it is necessary for market entry, promoting effective competition and improving social welfare. Therefore, it would be very desirable to provide ready access to big data, allowing every market player to achieve compatibility, technical upgrades and creation of new products and services. Therefore, the biggest challenge to maximizing the utility of big data is how to encourage data controllers to provide access to their data while preserving their incentives in collecting, processing, analyzing and exploiting big data. To facilitate access to data, the possibilities of establishing a data-trading market and an open platform for data controllers to upload their data, which would be accessible to service providers or even to the general public, must be explored. Some identified problems such as the lack of interoperability and standardization as well as pricing of data should be taken into consideration when establishing the market and the platform.[37]

In addition, de facto big data controllers might reach a market position that would propel them to refuse to license their actual and potential competitors to access and use big data they control.[38] It is quite clear that law should only force data controllers to provide access to big data they control when they reach a dominant market position and voluntary licensing negotiation with reasonable terms and conditions to access has failed after a reasonable period of time. In other words,

---

[35] See Max Planck Institute for Innovation and Competition, Position Statement on the European Commission's Public consultation on Building the European Data Economy, para. 8-16, available at SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2959924. However, if technical progress makes it possible for others to copy or use the encrypted data without authorization from data controllers, they would lose such excludability. Data would fall into the scope of public goods, and market failure would appear.

[36] See Josef Drexl, Designing Competitive Markets for Industrial Data -- Between Propertization and Access, Max Planck Institute for Innovation and Competition, Munich 2016, Max Planck Institute for Innovation and Competition Research Paper No. 16-1. See also Wolfgang Kerber, A New (Intellectual) Property Right for Non-Personal Data? An Economic Analysis (October 24, 2016), Gewerblicher Rechtsschutz und Urheberrecht, Internationaler Teil (GRUR Int), 11/2016, 989-999, available at SSRN: https://ssrn.com/abstract=2858171.

[37] The European Commission addressed in 2015 the problem of legal and technical barriers to the free flow of data (e.g. through interoperability and standardisation) in its communication, A Digital Single Market Strategy for Europe, COM (2015) 192 final, 6 May 2015, p. 15. See also Wolfgang Kerber, A New (Intellectual) Property Right for Non-Personal Data? An Economic Analysis (October 24, 2016), Gewerblicher Rechtsschutz und Urheberrecht, Internationaler Teil (GRUR Int), 11/2016, 989-999, pp. 14-20, available at SSRN: https://ssrn.com/abstract=2858171.

[38] Max Planck Institute for Innovation and Competition, Position Statement on the European Commission's Public consultation on Building the European Data Economy, paras. 28-30, available at SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2959924. See also Max Planck Institute for Innovation and Competition, Position Statement on Data Ownership and Access to Data, para. 39.

compulsory access to big data should be reserved as the last resort to ensure access that would render innovation and market competition more possible. If public interest is a key factor in the issue of access to big data, the question of how royalties should be calculated can be answered more easily.

2.3. Reconciling free cross-border data flow with data localization and data sovereignty

Trans-border flow and trading of big data through data collectors and brokers are happening in a big way. According to one study, cross-border data flows grew by 45 times between 2004 and 2014 and generated $2.8 trillion in global economic revenue in 2014 alone.[39] Having realized that big data has become a critical strategic resource for propelling innovation and competition, many countries have enacted laws and regulations to exert various forms of control over storage, cross-border transfer of data and localization of data.[40] For those countries cyberspace sovereignty or data sovereignty is also a big issue. In contrast, the US is pushing for the most liberal approach to advocate free cross-border data flow. Following the spirits of the two regulations discussed in 2.3.2., the EU should be basically singing the same tune as the US when data is being transferred cross the EU borders, but it has reservations with regards to personal data.

2.3.1. Under FTAs involving the US

The US supports the elimination of barriers to data flow as much as possible.[41] The US has already done so in the 2012 US-Korea FTA. The US-Korea FTA for the first time provides for the free flow of data and demands that parties "shall endeavor to refrain from imposing or maintaining unnecessary barriers to electronic information flows across borders.[42]" In the Trans-Pacific Partnership Agreement (TPP) negotiation, the US has succeeded in including in the "electronic commerce" chapter binding clauses that mandate contracting parties to allow cross-border data flow and prohibit data localization requirements, including the setting up or using of local computing facilities.[43] However, the TPP includes an exemption in Article 14.13(3) from the anti-data

[39] See New Zealand Ministry of Foreign Affairs & Trade, WTO e-commerce negotiations, https://www.mfat.govt.nz/en/trade/our-work-with-the-wto/wto-e-commerce-negotiations/

[40] For example, Russia's Data Localization Law requires all operators—both local and foreign—that possess the personal data of Russian citizens to use databases located exclusively in Russia and disclose the address of those data centres to Russian authorities. Brazilian Civil Rights Framework for the Internet (Marco Civil da Internet, Law No 12.965) states that data collected, stored, retained, or treated in Brazil shall respect Brazilian law. Even though it does not contain an explicit data localization requirement, it implies that certain data stored overseas by foreign companies might be subject to Brazilian law. In February 2014 India proposed significant new restrictions on cross-border data flows, including a requirement that all communications between users in India must stay in India and be stored locally on Indian servers. For more data-localization policies of other countries, see ITIF, Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost? https://itif.org/publications/2017/05/01/cross-border-data-flows-where-are-barriers-and-what-do-they-cost

[41] According to USITC, Global Digital Trade 1: Market Opportunities and Key Foreign Trade Restrictions (2017), p. 278, the data localization requirement "has forced companies to leave specific markets and could impede the development of information technology."

[42] Article 15.8, Chapter 15 of the US-Korea FTA provides that "Recognizing the importance of the free flow of information in facilitating trade, and acknowledging the importance of protecting personal information, the Parties shall endeavor to refrain from imposing or maintaining unnecessary barriers to electronic information flows across borders."

[43] Article 14.11.2 of the TPP provides "Each Party shall allow the cross-border transfer of information by electronic means, including personal information, when this activity is for the conduct of the business of a

localization requirement provided that the law achieves “a legitimate public policy objective,” and that the measure:(a) is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade; and (b) does not impose restrictions on the use or location of computing facilities greater than are required to achieve the objective. These clauses have been taken over by the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) after the US withdrew from TPP, which came into effect on 30 December 2018.[44] However, exception foreseen by Article 14.13(3) of the TPP is lacking in the USMCA.

2.3.2. Under EU regulations

The EU distinguishes between personal and non-personal data when dealing with data mobility within the EU. For personal data, the General Data Protection Regulation (GDPR) stipulates that "the free movement of personal data within the Union shall neither be restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data" (Article 3(1)). However, the GDPR requires that any entity transferring EU personal data out of the EU must make sure that such data still enjoy the same level of protection as it gets under Article 44.[45] In other words, any non-EU company that receives the personal data is under a legal obligation to follow GDPR data protection principles or their equivalent. This principle also applies to a controller or processor not established in the EU, where the data processing activities are related to: a) the offering of goods or services to data subjects in the EU; or b) the monitoring of data subjects’ behaviour as far as their behaviour takes place within the EU, however regardless of whether the control or processing takes place in EU or not.[46]

For the mobility of non-personal data within the EU, the EU has adopted the EU Regulation 2018/1807 on a Framework for the Free Flow of Non-Personal Data on November 14, 2018 (effective since May 2019), which creates a framework for the free flow of electronic non-personal data. In particular, the regulation prohibits data localization requirements, which means any obligation, prohibition, condition, limit or other requirement that imposes the data processing in the territory of a specific Member State or hinders the data processing in any other Member State. Over 60 such restrictions were identified in 25 jurisdictions within the EU and shall be repealed by 30 May 2021.[47] An exception to the general prohibition applies where data localization restrictions are justified on grounds of public security in compliance with the principle of proportionality.[48]

---

covered person”. Article 14.13.2 thereof provides that “No Party shall require a covered person to use or locate computing facilities in that Party’s territory as a condition for conducting business in that territory.”

[44] Article 1.1 of the CPTPP provides “The Parties hereby agree that, under the terms of this Agreement, the provisions of the Trans-Pacific Partnership Agreement, done at Auckland on 4 February 2016 are incorporated, by reference, into and made part of this Agreement mutatis mutandis……”

[45] Australia also requires an entity which sends personal data to an oversea recipient to make sure the recipient does not breach the Australian Privacy Principles (APPs) in relation to the information, and the entity is accountable for any acts or practices of the overseas recipient in relation to the information that would breach the APPs.

[46] Article 3.2 of the GDPR provides that “This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to: a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or b) the monitoring of their behaviour as far as their behaviour takes place within the Union.

[47] See Article 4(3), EU Regulation 2018/1807 on a Framework for the Free Flow of Non-Personal Data.

[48] See Article 4(1), EU Regulation 2018/1807 on a Framework for the Free Flow of Non-Personal Data.

2.3.3. Under Chinese regulations

China set up the Cyberspace Administration of China (CAC) directly under the State Council in 2014, which is the central Internet regulator, censor, oversight, and control agency for the PRC, and enacted its Cybersecurity Law in 2016, effective since June 1, 2017. This is the first of its kind in major jurisdictions.[49] The law is the latest step in China's campaign for jurisdictional control over data on the Internet.[50] It requires network operators to store select data within China and empowers Chinese authorities to conduct on-the-spot checks of a company's network operations.[51] The law has raised concerns among foreign companies over far-reaching data control as well as increased risks of IP theft.[52] The CAC issued in June 2019 a draft "Regulations on Assessing the Security of Transferring Personal Data out of the Country" for public consultation for one month. The Regulations require domestic Internet operators, which offer personal data that they have collected in the PRC to any entity outside of the country, to undergo security assessment with the provincial cyberspace department (Article 3). Personal data, the transfer of which out of the country might affect national security or damage public interest, or which lacks effective protection, may not leave the country (Article 2).

2.3.4. Under the WTO

Clearly there are huge differences between the approaches to big data adopted by the US, EU and China. The WTO is best poised to mediate and has launched at the eleventh WTO Ministerial Conference in Buenos Aires an e-commerce initiative on December 13, 2017, which was co-chaired by Japan, Singapore and Australia. Ministers from the three countries further co-hosted an informal meeting of Ministers on the WTO's e-commerce initiative on January 25, 2019 in the margins of the

[49] In the US, according to https://en.wikipedia.org/wiki/Cyber-security_regulation#Federal_government, there are few federal cybersecurity regulations, and the ones that exist focus on specific industries. The three main cybersecurity regulations are the 1996 Health Insurance Portability and Accountability Act (HIPAA), the 1999 Gramm-Leach-Bliley Act, and the 2002 Homeland Security Act, which included the Federal Information Security Management Act (FISMA). The three laws mandate that healthcare organizations, financial institutions and federal agencies should protect their systems and information. For example, FISMA, which applies to every government agency, "requires the development and implementation of mandatory policies, principles, standards, and guidelines on information security." However, the regulations do not address numerous computer-related industries, such as Internet Service Providers (ISPs) and software companies. Furthermore, the regulations do not specify what cybersecurity measures must be implemented and require only a "reasonable" level of security. The vague language of these laws leaves much room for interpretation.

[50] Article 1 stipulates "This Law is developed for the purposes of guaranteeing cybersecurity, safeguarding cyberspace sovereignty, national security and public interest, protecting the lawful rights and interests of citizens, legal persons and other organizations, and promoting the sound development of economic and social informatization."

[51] Article 8 of the Cybersecurity Law of China demands that "The national cyberspace administration shall be responsible for the overall planning and coordination of cybersecurity work and relevant supervision and administration." Article 37 requires that personal information and important data collected and produced by critical information infrastructure operators (those whose business relates to public communications and information services, energy, transport, water conservancy, finance, public services and e-government affairs, etc.) be stored within China, and if it is indeed necessary to provide such information and data to overseas parties due to business requirements, security assessment shall be conducted in accordance with the measures developed by the national cyberspace administration.

[52] The Diplomat, China's Cybersecurity Law: What You Need to Know, https://thediplomat.com/2017/06/chinas-cybersecurity-law-what-you-need-to-know/

World Economic Forum Annual Meeting in Davos, Switzerland.[53] Following the meeting, 76 WTO Members (including the EU, the US and China) representing over 90 percent of global trade issued a Joint Statement on Electronic Commerce. According to the Joint Statement, "We confirm our intention to commence WTO negotiations on trade-related aspects of electronic commerce. We will seek to achieve a high standard outcome that builds on existing WTO agreements and frameworks with the participation of as many WTO Members as possible".[54] There is still a long way to go before a new world trade order that is premised on a functional global governance on the exploitation of big data under the WTO can be ushered in. Nevertheless, China has recently changed its conservative stance on this issue and signed the Joint Statement.

3. Algorithms and challenges they pose

In mathematics and computer science, an algorithm is an unambiguous specification of how to solve a class of problems. Algorithms can perform tasks such as calculation, data processing, and automated reasoning.[55] Algorithms decide how computers and AI work as well as how big data are being collected, make decisions on online trading (search, pricing, and terms and conditions), reputation, and financing, independent of humans, and even develop patterns human cannot detect. With the help of big data, a machine can improve itself by preset and adjustable algorithms, such as machine learning (ML) algorithms, and help consumers make decisions and promote their welfare.[56] However, algorithms do not provide information about their internal decision-making process, and are therefore often described as a black box.[57] Taking Google for example, it rose to the top of the tech pack while zealously guarding its "secret sauce"—the complex algorithms.[58] However, the same complex algorithms were also secretively used by Google to systematically favor its own comparison shopping service (Google Shopping), and caused harm to its competitors, such as TripAdvisor and Expedia.[59]

3.1. Algorithm as one-way mirror

Algorithms, being a black box or one-way mirror, are posing challenges to our data-driven economy. For one thing, algorithms, if not correctly designed, can collect and process data beyond the original purpose for which the data is collected and used for. Such use may well be contrary to the principle

[53] See Minister for Trade, Tourism and Investment: Australia, Japan and Singapore welcome WTO electronic commerce negotiations, https://trademinister.gov.au/releases/Pages/2019/sb_mr_190126a.aspx

[54] See WTO Joint Statement on Electronic Commerce (WT/L/1056); see also Bloomberg, China to Join Talks on $25 Trillion E-Commerce Market at Last Minute, https://www.bloomberg.com/news/articles/2019-01-25/china-is-said-to-join-global-e-commerce-talks-at-last-minute

[55] See Wikipedia, Algorithm, https://en.wikipedia.org/wiki/Algorithm

[56] See Lilian Edwards & Michael Veale, Slave to the Algorithm: Why a Right to an Explanation Is Probably Not the Remedy You Are Looking for, 16 Duke L. & Tech. Rev. 18, p. 19 (2017-2018).

[57] See Sandra Wachter, Brent Mittelstadt and Chris Russell, Counterfactual Explanations Without Opening the Black Box: Automated Decisions and the GDPR, Harvard Journal of Law & Technology, 31 (2), 2018, p. 3, available at SSRN: https://ssrn.com/abstract=3063289

[58] Frank Pasquale, The Black Box Society—Secret Algorithms That Control Money and Information, p. 13.

[59] On 27 June 2017 the EC reached the conclusion that Google abused its dominance in the general internet search market in 13 members of European Economic Area (EEA) by positioning and displaying more favorably on its general search results pages its own comparison shopping service, which led to a sharp increase of traffic to Google's websites (45 times in the UK, 35 times in Germany, 19 times in France, and 29 times in the Netherlands). The EC imposed the highest ever fine of Euro 2.42 billion on Google.

of data protection under the GDPR, i.e., data should only be collected for named and specific purposes.[60] This is a common practice by Internet companies, which may benefit consumers to an extent but also bring harms to them. Take personalized online shopping, or targeted online marketing, as an example. On the one hand, it reduces the bewildering options for consumers, and saves them time and efforts to locate what best meets their demand. On the other hand, however, it also shapes consumers' preferences, subjects them to a monotonous consumption pattern especially when they are willing to buy something outside their past choices, and makes first-degree price discrimination a reality to maximize profits.[61]

For another, it is extremely difficult to verify whether algorithms are as scientific and neutral (bias-free) as some internet giants allege. Former CEO of Google Eric Schmidt once told a scary story of how this one-way mirror works in 2010: 'With your permission you give us more information about you, about your friends, and we can improve the quality of our searches, we don't need you to type at all. We know where you are. We know where you've been. We can more or less know what you're thinking about.[62]' Algorithms take in data about us and convert it into risk calculations, paid rankings and personalized recommendations that may have vitally important consequences for us, and yet are immune from scrutiny.[63] Facebook and WeChat decide who we are, Amazon and Jingdong decide what we want, Google and Baidu decide what we think, all because of algorithms, and we know nothing about them.[64] Those companies use the data to make important decisions about us and to influence the decisions we make for ourselves. If we cannot deal with the black box issue of algorithms, the opacity and complexity they now possess will continue to let deception, overpricing and fraud flourish.[65]

Consequently, national states are facing the serious challenge of how to audit algorithms of tech/online giants, such as Google, Facebook, Alibaba, Tencent (WeChat). One recent case in point is the keywords advertisement by Google in Taiwan. In this case, Google was selling "幸福空間" (Chinese characters, which can be roughly translated as "Happy Space") as keywords to advertisers so that they could promote their services in the search results page when users search on Google by keying "幸福空間" as the keywords. However, "幸福空間" is a registered trademark owned by the plaintiff and already recognized by Taiwan's IP Office as a well-known trademark. In 2015 Taiwan's IP Court held that Google's practice constituted unfair competition in violation of Article 25 of the Fair

[60] Article 5(1)(b) of the GDPR provides that "Personal data shall be: (b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes…('purpose limitation')"

[61] First-degree price discrimination, alternatively known as perfect price discrimination, occurs when a firm charges a different price for every unit consumed. The firm is able to charge the maximum possible price for each unit based on consumers' individual preferences and reservation prices to capture all available consumer surplus for itself. First-degree discrimination was once rare in practice, but has become a daily reality thanks to big data and AI. See https://www.economicsonline.co.uk/Business_economics/Price_discrimination.html

[62] See https://www.theatlantic.com/technology/archive/2010/10/googles-ceo-the-laws-are-written-by-lobbyists/63908

[63] Frank Pasquale, The Black Box Society -- Secret Algorithms That Control Money and Information, Harvard University Press 2015, p. 4.

[64] George Dyson, Turing's Cathedral: The Origins of the Digital Universe (New York: Pantheon, 2012), 308.

[65] Frank Pasquale, The Black Box Society—Secret Algorithms That Control Money and Information, Harvard University Press 2015, p. 15.

Trade Act,[66] without committing trademark infringement, as there was no trademark use in the context of keyword advertisement. Taiwan IP Court awarded triple damages, which is a rarity, of NT$67,146 (about US$2,100) based on a profit of NT$22,382 conceded by Google.[67] However, the court was powerless to verify the amount Google conceded and to monitor whether Google has indeed ceased its faulted practice.

China has the most daunting challenge of how to reign in dominant search engine operators' abusive algorithms. Baidu, a notorious internet giant in China, owns 62.09% market share in the Chinese search engine industry,[68] and has long been suspected of giving self-serving results to favor Baidu's eco-system,[69] and yet no investigation has ever been launched against it. One recent example of Baidu's rotten practice is the shocking promotion of its own product, Baijiahao, a blog-style platform introduced in 2016 for independent writers, bloggers, and journalists to post news and share works. Baidu displays Baijiahao with enhanced features at or near the top of the first general search page even though it contains non-relevant data.[70] Such conduct diverts the traffic from Baidu's general search results pages to Baijiahao and puts competing products in a less noticeable position. One possible reason for the inaction of Chinese law enforcement agency is that it has no clue of how to audit those algorithms Baidu used to conduct abusive behaviors.[71] This brings us to the next important issue.

3.2. How can algorithms be audited?

As algorithms, particularly ML algorithms, are increasingly important for our daily lives, concerns over the unfairness, discrimination and opacity of algorithms also arise. More and more, calls for algorithmic transparency are being voiced and heard in public discourse.[72] But how can we audit algorithms? One fundamental principle to follow is that any kind of auditing must aim to carefully balance the goal of correcting identified negative effects of algorithms, such as opacity,

[66] Article 25 of the Taiwanese Fair Trade Act is a general clause prohibiting deceptive and unfair trade practice: "In addition to what is provided for in this Act, no enterprise shall otherwise have any deceptive or obviously unfair conduct that is able to affect trading order."

[67] See Taiwan IP Court 2013 Min-Shang-Shang-Zi 8 (decided on 12 February 2015). For discussion of the decision, see Kung-Chung Liu, 2.2. Google's Keyword Advertisement in Taiwan Did Not Constitute Use of Trademark, but Obviously Unfair Practice, in Kung-Chung Liu (ed.), Annotated Leading Trademark Cases in Major Asian Jurisdictions (Routledge forthcoming 2019).

[68] See http://gs.statcounter.com/search-engine-market-share/all/china (Feb. 2018 – Mar. 2019)

[69] For Baidu's questionable behaviors in recent years, see https://medium.com/@yihongpoo/baidu-is-dead-tech-companies-and-fake-news-in-china-e68ff3cfa184

[70] According to Fang Kecheng, as of the morning of Jan. 22, 2019 four of the top five results for a query on China's GDP report were Baijiahao articles, yet not a single one of them contained the relevant data. See http://www.sixthtone.com/news/1003497/how-baidu-learned-to-stop-worrying-and-love-the-walled-garden

[71] One source suggests that the reason why Baidu is able to manipulate the search results to give itself an unfair advantage without being investigated by Chinese government is that it acts in tandem with the latter to make judgement on free speech and misinformation. See https://medium.com/@yihongpoo/baidu-is-dead-tech-companies-and-fake-news-in-china-e68ff3cfa184

[72] Omer Tene & Jules Polonetsky, Big Data of All: Privacy and User Control in the Age of Analytics, 11 Nw. J. Tech. & Intell. Prop. 239, pp. 268-272 (2013).

discrimination and unfairness, with the goal of not stifling innovation and not offsetting the beneficial effects of big data and algorithms for businesses, consumers, and society as a whole.[73]

One approach to audit algorithms is to examine the algorithms at issue. In the Google comparison shopping case in the EU, the EC has gone through a detailed audit on Google's algorithms, although it withheld much valuable information about auditing to protect Google's trade secrets.[74] The EC collected and analyzed contemporary documents of Google and its competitors: 5.2 terabytes (TB =1024GB) of data, including 1.7 billion actual searches with Google.[75] Google was found to have used discriminatory algorithms. More specifically, the position and display of Google's comparison shopping services and its competitors' in Google's general search results pages are treated unequally by Google. The EC explains how Google managed to do so. As for the position, Google uses dedicated algorithms, as opposed to normal generic ones,[76] to identify and demote competing comparison shopping services in Google's general search results,[77] reducing their ranking and visibility drastically. Google uses at least two kinds of dedicated algorithms to conduct anti-competitive practices, and only one has been disclosed, with the other being anonymized. The disclosed one, Panda, was introduced in the US in February 2011, then subsequently extended to all English language queries worldwide on April 11, 2011 and to all general search queries across the EEA on August 12, 2011. The visibility of most important comparison shopping services in Google's general search results pages dropped suddenly after the launch of the Panda algorithm in the respective EEA country.[78] As for the display, competing comparison shopping services can be displayed only as generic search results in Google's general search results pages, and therefore cannot be displayed in rich format with pictures and additional information on the products and prices, which would definitely increase click-through rates.[79] In contrast, Google's own comparison shopping service is prominently positioned, and displayed in rich format by those algorithms.[80]

[73] See Gerhard Wagner and Horst Eidenmüller, Down by Algorithms? Siphoning Rents, Exploiting Biases and Shaping Preferences – The Dark Side of Personalized Transactions (March 30, 2018), University of Chicago Law Review, Forthcoming; Oxford Legal Studies Research Paper No. 20/2018, p.2, available at SSRN: https://ssrn.com/abstract=3160276 or http://dx.doi.org/10.2139/ssrn.3160276.

[74] See, e.g., Case AT 39740, paras.349-396.

[75] See Sections 7.2 and 7.3 of Case AT 39740—Google Search (Shopping).

[76] The function of such algorithms can be summarized as follows: when a user searches on Google, in response to the user query in Google's general search engine, generic search algorithms are used to rank web pages, including those of competing comparison shopping services. These algorithms include the PageRank algorithm. Google also applies a variety of adjustment mechanisms to the results of the PageRank algorithm "to improve the user experience". See Case AT 39740, para. 345.

[77] See Case AT 39740, para. 359.

[78] See Case AT 39740, paras. 356 and 361.

[79] See Case AT 39740, paras. 371-372.

[80] See Case AT 39740, paras. 344 and 379. This abusive conduct helped Google divert traffic by decreasing traffic from Google's general search results pages to competing comparison shopping services and increasing traffic from Google's general search results pages to Google's own comparison shopping service, and thus has anti-competitive effects on comparison shopping services and general search services in the national markets of EEA. See Case AT 39740, para. 341.

The second suggested approach is that auditing algorithms does not require the disclosure of source code, including the model and inputs and outputs of training set data.[81] Doing so, as suggested by Kroll et al., is neither necessary to, nor sufficient for, algorithmic accountability. Moreover, it may cause self-harm in terms of privacy disclosure and the creation of "gaming" strategies, which can subvert the algorithm's efficiency and fairness. As an alternative, they point out that auditing, both in the real and the digital world, can achieve algorithmic accountability by looking at the external inputs and outputs of a decision process, rather than at the inner workings.[82]

A third possible avenue, attractive at least to some, to solving the problem of transparency could be to allow the exercise of the "right to an explanation" of algorithmic decision-making under the GDPR.[83] The GDPR establishes a number of safeguards designed to ensure the "fair and transparent processing" of personal data, including an obligation that entities provide "meaningful information about the logic involved" in certain types of highly automated decision-making systems. The rights of data subject that mandate disclosure of "meaningful information" are collectively referred to as "the right to an explanation." Even though it is designed as a means to opening the "black box" of algorithms, it is probably not a workable solution, due simply to the fact that it can only be applied to some but not all personal data, and its language can hardly be stretched to be applied to highly multidimensional ML algorithms.[84]

In the area of competition law, algorithms may foster tacit collusion, adversely affecting consumer choice, and even posing a threat to pluralism. In particular, algorithm-driven market interactions call traditional economic models into question (explicit v. tacit collusion). It is still unclear whether and how the new challenges can be addressed within the existing framework of competition law or whether new legal tools, such as algorithm-focused regulation, must be developed.[85]

3.3. How can we build creditable auditing bodies for algorithms?

3.3.1. A new treaty

Within national borders, some scholars try to explore the possibilities of building an external regulator or audit body, whose functions include investigating complaints and providing mediation or adjudication. Andrew Tutt analyzed the analogy between drugs and algorithms, and concluded that an agency like the US Food and Drug Administration (FDA) is feasible and that certain classes of

[81] The idea of using training set data in machine learning programs is a simple concept, but it is also very foundational to the way that these technologies work. The training set data is an initial set of data used to help a program understand how to apply technologies like neural networks to learn and produce sophisticated results. It may be complemented by subsequent sets of data called validation and testing sets. See Techopedia, Training Data, https://www.techopedia.com/definition/33181/training-data.

[82] See Joshua Kroll et al., Accountable Algorithms, 165 U. PA. L. REV. 633, 654 (2017).

[83] See Bryce Goodman & Seth Flaxman, EU Regulations on Algorithmic Decision Making and "a Right to an Explanation," ICML WORKSHOP ON HUMAN INTERPRETABILITY IN ML (2016); see also Articles 13(2)(f), 14(2)(g), 15(1)(h) and 22 of the GDPR.

[84] See Lilian Edwards & Michael Veale, Slave to the Algorithm: Why a Right to an Explanation Is Probably Not the Remedy You Are Looking for, 16 Duke L. & Tech. Rev. 18, pp. 18-19 (2017-2018).

[85] Peter Georg Picht and Benedikt Freund, Competition (law) in the era of algorithms, Max Planck Institute for Innovation and Competition Research Paper No. 18-10, available at SSRN: https://ssrn.com/abstract=3180550

new algorithms should not be permitted to be distributed or sold without its approval.[86] Crawford and Schultz, by proposing to grant individuals a right to procedural data due process to mitigate predictive privacy harms, argue the US Fair Trade Commission (FTC) could work as a neutral data arbiter to routinely examine big data providers.[87] A European-style ombudsman body such as the Data Protection Authority (DPA) of each member state, which handles complaints lodged against violations of the GDPR, might also be a suitable auditor, as it could be equipped with technical expertise necessary to understand and police algorithmic harms.[88] National public authorities can impose certain kinds of obligation on internet companies, such as to disclose to consumers the application of first-degree price discrimination.[89]

However, who should be the trusted auditors for international auditing of algorithms?[90] Self-regulation by tech companies alone has proven to be futile. E-commerce platforms such as Amazon and Jingdong have been concealing their preference-shaping algorithms from their customers. Facebook is also one case in point. One latest testament to this is a report from British lawmakers that finds that Facebook and other big tech companies were failing their users and dodging accountability.[91] Likewise, consumers' unassisted self-help can be of limited help, as they are at a knowledge disadvantage and mostly do not understand how algorithms work. Refusal to grant internet companies collection of personal data while using their products or service, such as disallowing tracking cookies, or utilizing technological tools to make themselves anonymous, could help them withhold such data, but also risks them being shut out of transactions with certain firms or even important segments of the market.[92]

It is therefore worth discussing how to empower a third-party agency or organization to provide auditing service. Any national public authorities would be an ill fit, as algorithms of major online companies could mean the national competitiveness of the country where they headquarter. The

[86] Tutt also proposes that the agency should serve as a centralized expert regulator that develops guidance, standards, and expertise in partnership with industry to strike a balance between innovation and safety. See generally Andrew Tutt, An FDA for Algorithms, 69 ADMIN. L. REV. 83, 119-123 (2017).

[87] See Kate Crawford & Jason Schultz, Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms, 55 B.C. L. REV. 93, 127 (2014).

[88] Admittedly, national DPAs are already struggling to regulate general privacy issues, and would therefore be stretched to their limits to regulate these more complex algorithmic harms to society. See Lilian Edwards & Michael Veale, Slave to the Algorithm: Why a Right to an Explanation Is Probably Not the Remedy You Are Looking for, 16 Duke L. & Tech. Rev. 18, 58-62 (2017-2018).

[89] The House of Lords (Select Committee on European Union) in the UK has specifically recommended in the 2016 "Online Platforms and the Digital Single Market" report (para. 291) that "online platforms be required to inform consumers if they engage in personalized pricing." See https://publications.parliament.uk/pa/ld201516/ldselect/ldeucom/129/129.pdf.

[90] Frank Pasquale, The Black Box Society—The Secret Algorithms That Control Money and Information, Harvard University Press 2015, p. 141.

[91] See National Public Radio, Facebook Has Behaved Like 'Digital Gangsters,' U.K. Parliament Report Says, https://www.npr.org/2019/02/18/695729829/facebook-has-been-behaving-like-digital-gangsters-u-k-parliament-report-says.

[92] See Gerhard Wagner and Horst Eidenmüller, Down by Algorithms? Siphoning Rents, Exploiting Biases and Shaping Preferences – The Dark Side of Personalized Transactions (March 30, 2018), University of Chicago Law Review, Forthcoming; Oxford Legal Studies Research Paper No. 20/2018, pp. 7-8, available at SSRN: https://ssrn.com/abstract=3160276 or http://dx.doi.org/10.2139/ssrn.3160276.

intervention by any specific national agency could easily lead to mistrust. We believe that a public-private partnership under multilateralism would be more preferable and plausible. Countries, including both the US and China, are advised to work under the umbrella of the WTO and to reach a new World Algorithm Treaty (WAT) in the context of e-commerce negotiation.

3.3.2. A global public-private partnership agency

The World Algorithms Council (WAC), which will be in charge of the administration of the WAT, should follow the model of the International Telecommunication Union (ITU),[93] with its current membership of 193 countries and over 800 private-sector entities and academic institutions, to include multiple stakeholders, especially algorithm giants. First steps for the WAC to take would probably be setting up standards for classifying algorithms by varying levels of regulatory scrutiny based on the complexity of the algorithms. Drawing on best practices from other sectors may well help solve the algorithmic problem we are facing. Health care, for example, is a sector closely related to public interests. For this reason, "regulators are deploying technologically savvy contractors to detect and deter fraud, abuse, and unnecessary treatments".[94] Similar techniques can and should also be used to regulate banks, search engines and social networks whose businesses are also strongly associated with public interests. Public interests thus can play an important role in the use of algorithms or data. Therefore, also needed is the setting up of common parameters that include "public values" and "public interests" in the design of algorithms to keep the operation of algorithms honest.

The WAC then needs to establish guidance for testing and performance to ensure that algorithms are developed with adequate neutrality (free of biases and competitive advantages) and margins of safety, further to establish satisfactory measures of predictability and explainability, and finally to distribute liability for harm among coders, implementers, distributors, and end-users.[95] As suggested by the AI Now 2017 Report, "Ethical codes meant to steer the AI field should be accompanied by strong oversight and accountability mechanisms".[96] After putting in place the above-mentioned mechanisms, the WAC would be an ideal auditor for auditing algorithms. If Internet giants fail to disclose their algorithms in question to the WAC for auditing, the WAC should be empowered to take actions against them, such as advising the public to avoid such algorithms and reminding the public of possible dangers associated with them.

4. Conclusion

According to Thomas Friedman, this trade war can end well only if China is honest about all the pillars of its formula for success (hard work, unfair competition, and a stable world order built by the US) and if Trump is honest about all of the US: education, best infrastructure (roads, ports, airports

---

[93] The ITU is a treaty organization founded under the aegis of the United Nations, and one of its responsibilities is to develop telecom standards to ensure networks and technologies seamlessly interconnect; see https://www.itu.int/en/about/Pages/default.aspx; see also Rudi Bekkers and Andrew Updegrove, A Study of IPR Policies and Practices of a Representative Group of Standards Setting Organizations Worldwide (September 17, 2012), pp. 15-16, available at SSRN: https://ssrn.com/abstract=2333445.

[94] According to Frank Pasquale, the US state officials closely monitor reputational intermediaries, requiring key "doctor rating" sites to disclose the data they use and the way they analyze it. New health privacy regulations have also focused on an "accounting of disclosures" that should help patients understand how data about them is compiled and disseminated. Frank Pasquale, The Black Box Society -- Secret Algorithms That Control Money and Information, Harvard University Press 2015, p. 16.

[95] See generally Andrew Tutt, An FDA for Algorithms, 69 ADMIN. L. REV. 83, 107-109 (2017).

[96] AI Now 2017 Report, p. 2, available at: https://ainowinstitute.org/AI_Now_2017_Report.pdf

and telecom), the most government-funded basic research, the best rules and regulations to incentivize risk-taking and prevent recklessness, and the most open immigration system.[97] However, we are of the opinion that big data, algorithms and the US-China trade war are closely intertwined, and we cannot really solve the one question, without solving the other two at the same time. The US-China trade war may find an interim truce whenever some agreement has been reached. But it can easily reignite, so long as issues related to big data and algorithms are not solved by a new world trade order through the help of a new international treaty.

Before that grand plan can be realized, the whole world is looking to China to take the right steps towards finding a lasting solution, which could include:

1. Opening its Internet and telecommunication markets to the rest of the world, including the US, to allow data giants such as Amazon, Google, Facebook, and Twitter back into China to compete fairly with their Chinese counterparts like Baidu, Alibaba, JD and Tencent. It is only fair for China to do so, and wise too, as it will save Chinese people from servitude to the likes of Baidu.
2. Saying no to a fragmented world of internets and IOTs along the dividing line between the US camp and the China camp (such as B&R countries), as this would be a disaster for humankind.
3. Taking the Joint Statement it recently signed seriously and showing its commitment in the upcoming e-commerce negotiation under the WTO framework.

Last but not least, we, citizens of the globe, should join hands to turn this ugly trade war into a golden opportunity for building a new world trading order suited for the data-driven economy.

[97] See Thomas Friedman: China and Trump, Listen Up!, https://www.nytimes.com/2018/11/13/opinion/china-trump-trade.html