CWS/WP/200/37

WORKING PAPER

TRADE RULES ON SOURCE CODE- DEEPENING THE DIGITAL INEQUITIES BY LOCKING UP THE SOFTWARE FORTRESS

NEERAJ R.S.

April 28 2017

Centre for WTO Studies

Indian Institute of Foreign Trade

TABLE OF CONTENTS

I. INTRODUCTION

TRADE RULES ON SOURCE CODE: SOME RECENT DEVELOPMENTS

At the second Ministerial Conference of the World Trade Organization (WTO) at Geneva, members to the WTO adopted a "Declaration on Global Electronic Commerce" which called for the establishment of a comprehensive work programme to examine all trade-related issues relating to global electronic commerce including those issues identified by Members.[1] Although the mandate is limited to "examining all trade-related issues relating to global electronic commerce", since 2016 there has been a palpable growth in the pressure exerted by a select few members to start negotiations on e-commerce at the WTO. Several proposals have been submitted by WTO members suggesting possible elements for a multilateral rule book on trade-related aspects of e-commerce.

A proposal that is contained in some of these submissions calls for disciplines for "protecting source code". A non-paper submitted by the United States outlining a work programme on electronic commerce contains the following proposal:

2.7. *PROTECTING CRITICAL SOURCE CODE: Innovators should not have to hand over their source code or proprietary algorithms to their competitors or a regulator that will then pass them along to a State-owned enterprise. It is important to ensure that companies do not have to share source code, trade secrets, or substitute local technology into their products and services in order to access new markets while preserving the ability of authorities to obtain access to source code in order to protect health, safety or other legitimate regulatory goals.* [2]

Japan's proposal contains elements on disclosure of important information such as trade secrets including source code: "*The disclosure of important information, such as trade secrets including source code, should not be a condition for the import, distribution, sale or use of related products including digitally encoded products in Member's territory.*"[3] The proposal from Canada, Chile, Colombia, Cote d'Ivoire, European Union, Korea, Mexico and Singapore prescribes a series of measures to ensure a "given level of openness in

[1]WT/MIN(98)/DEC/2, "Declaration on Global Electronic Commerce", *World Trade Organization,* Ministerial Conference, Geneva, 1998.
[2]JOB/GC/94, "Non-Paper from the United States," Work Programme on Electronic Commerce, *World Trade Organization*, July 2016.
[3] JOB/GC/100, "Non-Paper from Japan," Work Programme on Electronic Commerce, *World Trade Organization*, July 2016.

e-commerce markets. It proposes "*measures to refrain from requirements on the transfer of or access to, source code of software, as a condition of market access*".[4]

Rules that prohibit governments from requiring the disclosure of source code have already made it into Regional Trade Agreements (RTAs) such as the Trans-Pacific Partnership (TPP) and Japan-Mongolia Economic Partnership Agreement (EPA) and the on-going plurilateral negotiations such as the Trade in Services Agreement (TiSA).

Broadly, the proponents of these rules on source code are proposing that governments should be prohibited from requiring the transfer of, or access to, the source code of software programmes as a condition for market access. Several countries, both developing and developed, have implemented legislations and policies that require the source code of software applications used in education, health, defence sectors and government institutions to be open. In some other cases, countries are providing preferential treatment to softwares with open source code. The policy flexibility that is currently available for countries to impose open source code as a market access condition (or to provide preferential treatment to open source code) is being used or can be used to pursue objectives like security, economic development, preventing anti-competitive and deceptive practises and spurring indigenous innovation. More importantly, that Open Source Software (OSS) has better cost-efficiency and more innovative potential as compared to proprietary software is well established today. In light of this, it is important to develop a deep understanding of the implications of proposals on source code made at the WTO and disciplines contained in FTAs, along with exceptions (if any) contained therein, on the policy and regulatory space of countries and their pursuit of legitimate objectives. This is particularly important for developing countries that are still evolving their Information and Communications Technology (ICT) strategies and are keen on making them relevant for their development processes.

Before delving into the proposals and disciplines prohibiting state-required disclosure of software source codes and its implications for developing countries, it is important to first understand the concept of source code and the difference between Open Source Software (OSS) and Proprietary Software. Section II attempts to develop a conceptual understanding of source code and condenses the literature comparing the two types of software platforms- OSS and Proprietary Software. It traces the history of software production and attempts to argue why OSS has advantages over

[4] JOB/GC/97,"Non-Paper from EU et al," Work Programme on Electronic Commerce, *World Trade Organization*, July 2016.

proprietary software. Section III takes note of how the proposals for protection of source code will fit within the larger realm of multilateral trade disciplines (WTO rules) so as to assess potential conflicts between these proposals and extant WTO rules. Section IV analyses source code disciplines contained in FTAs, particularly the TPP and studies its implications on developing countries. Regulations requiring source code disclosures are in force in several developing countries. The proposal to develop global rules to prohibit or regulate the disclosure of source code is underpinned by the pressure exerted by commercial interests and lobby groups situated in advanced countries that seek unconditional market access for their technologies and technology-embedded products, while diminishing the use of OSS. Section V attempts to trace the genesis of the source code proposal to regulations on source code disclosure in developing countries and the push back from business groups against such regulations. Section VI concludes.

II. UNDERSTANDING SOURCE CODE

SOURCE CODE: BUILDING BLOCKS FOR MACHINE LANGUAGE

Source Code refers to the list of instructions that is written by a human programmer using programming languages (such as BASIC, C, C++, JAVA, Fortran) and forms the "recipe" for a software application[5]. They are written in human readable text language and are first converted into "object codes" by programmes known as compilers before the software can be used on a computer. Compiling is the process of converting the source code into binary code (series of ones and zeroes) after which it is saved as a separate file. The object code is finally assembled into an "executable code" that is understood and run by computers and other devices. Object codes and executable codes are in machine language (binaries) and cannot be "read" or understood by humans. Source code, therefore, represents the final point in the interface between humans and Information Technology (IT) devices. Access to source code is a pre-requisite for understanding and modifying the software that runs any IT device.

CATHEDRALS AND BAZAARS: UNDERSTANDING PROPRIETARY SOFTWARE AND OPEN SOURCE SOFTWARE

The source code of a proprietary or commercial software is accessible only to the producer of that software and are not accessible to the buyers of that software. Considered as good as a trade secret by its developer[6] most proprietary softwares are distributed only as executable binary files, which a human cannot read and therefore cannot modify. They are sold to be installed and used directly by the user without modification or customization apart from certain parameter settings. When purchasing such a software, the buyer subscribes to a right-to-use license which permits her to use the software on a device under the terms that she cannot reproduce it, modify it, improve it or redistribute her own version of the software to others.[7] The buyer will, in any case, not be able to do

[5]Mitchell L. Stoltz, "The Open Source Revolution: Transforming the Software Industry with Help from the Government," *Pomona Senior Theses*, No.7, 2.

[6] Mitchell Stoltz of Mozilla.org made the popular analogy of the source code of proprietary software to the formula of Coca Cola in "The Open Source Revolution: Transforming the Software Industry with Help from the Government," *Pomona Senior Theses*, No.7, 2.

[7]The License Terms of a typical Microsoft software contains the following terms: "This license does not give you any right to, and you may not: use or virtualize features of the software separately, publish, copy (other than any permitted backup copy), rent, lease, or lend the software; transfer the software (except as permitted by this agreement), attempt to circumvent technical protection measures in the software, reverse engineer, decompile, or disassemble the software,

any of these because she does not have access to the source code (reverse engineering the object code back to source code is generally not possible).

Open source software (OSS) is a computer software that is available in open-source code form. A software program that has an open source-code permits parties other than the original programmer to freely access the underlying source code of the programme. The source code of the software is released along with the binary files that run on the computer for the buyer/user to examine, use or modify it freely. It is important to note that "free" here does not mean that the price is necessarily zero. It connotes the "freedom" to run the programme, to study how it works and customize it to one's own needs, to redistribute copies to others and to improve the programme and share improvements with the community so that all benefit.[8] Essentially, by liberating the source code and expressly allowing the users to modify and redistribute it, OSS inverts the traditional Intellectual Property (IP)-like regime of proprietary software.

Such a model of free and open source begs several questions: considering that OSS is a "public good", why does it not disintegrate to the point where no one makes substantial contributions and the good never gets produced? Why would a user voluntarily contribute to a system that she could otherwise use as a free-rider?

It needs to be recognised that the organisational model of OSS is completely different from the normative organizational models that are adopted for producing an industrial good- it eschews a pre-determined division of labour that is managed by a corporate hierarchical structure, the notion of proprietary knowledge that is guarded by strong and enforceable IP rights and the ultimate motive of profit maximisation. The OSS model is developed and maintained in an entirely non-proprietary setting where programmers work in an unstructured and parallel manner and sometimes without a direct and immediate monetary return. Eric Raymond, in his widely cited book "Cathedrals and Bazaars", refers to OSS as a great babbling bazaar of differing agendas and approaches out of which a coherent and stable system could seemingly emerge only by a succession of miracles. This contrasts sharply with a 'cathedral' model which represents the hierarchically-organized, authoritatively ordered division of labour. What sustains the bazaar model of OSS,

---

except if the laws where you live permit this even when our agreement does not. In that case, you may do only what your law allows. When using Internet-based features, you may not use those features in any way that could interfere with anyone else's use of them, or to try to gain access to any service, data, account or network, in an unauthorized manner."

[8] The Free Software Definition, *Free Software Foundation (FSF)*, www.fsf.org/philosophy/free-sw.html, 1996

according to Raymond, is that highly motivated individuals[9] make "voluntary contributions as a reaction to abundance rather than scarcity, the abundance being that of knowledge and information as well as of network bandwidth and computing power".[10] Steven Weber gives a three step explanation for why anyone would want to produce OSS- motivations of individuals, the economic logic of a distinctive production process, and a set of social and political structures that maintain coordination and manage complexity.[11] The existence of OSS is also rationalised by the cooking pot model which suggests that it came about as a result of the distributed structure of the Internet where users do not want to pay or charge for goods and services that thrive on the internet.[12]

Instead of resorting to theoretical explanations, the sustainability of the OSS model could very well be demonstrated by the success of OSS projects. In the past few decades OSS model has had an impressive success in capturing market shares in the commercial software markets which has traditionally been highly concentrated (oligopolistic). In server operating system market, Linux, an open source operating system, holds more than a 30% share, and Microsoft's Windows holds approximately a 50% share. In web server market, more than 60% of websites use Apache (an open source software), but only about 30% use Microsoft's Internet Information.[13] Mozilla Firefox has almost completely displaced Microsoft's Internet Explorer as the most commonly used web browsers. Google Chrome is based on an open source project known as the "chromium project" which provides the code for Google Chrome. Some of the most widely used video players (VLC, Media Player Classic), anti-virus softwares and phone-based apps are developed on open source software.

A BRIEF HISTORY OF SOFTWARE PRODUCTION

Richard Stallman who initiated the Free and Open Source Software Project (FOSS) in the 1980s which led to establishment of Free Software Foundation (FSF) once quipped that the "sharing of

[9] A 2001 Survey conducted by Boston Consulting Group concluded that the motivations of individual developers can be segmented into four groups- One-third of the respondents were strongly motivated by the conviction that source code should be open. One fourth were "fun seekers" who code for intellectual simulation. One fifth are "professionals" and another one-fifth are "skill enhancers" who emphasised the learning and experience they get from OSS.

[10] Raymond ES, The Magic Cauldron, http://www.catb.org/esr/writings/magic-cauldron/ (accessed on 07.03.2017)

[11] Steven Weber, "The Political Economy of Open Source," *BRIE Working Paper* 140, E-conomy Projectä Working Paper, 15 June 2000.

[12] Ghosh RA, "Cooking pot markets: An economic model for the trade in free goods and services on the Internet," *First Monday,* 3 (3), 1998.

[13] L H Lin, "Impact of user skills and network effects on the competition between open source and proprietary software.," *Electronic Commerce Research and Applications*, Volume 7 Issue No.), 68-81; 2008

softwares is as old as computers... just as the sharing of recipes is as old as cooking itself."[14] In the early days (1960s) of software programming, software was bundled along with the hardware and was not seen as a means of making profit but as a hook to encourage people to buy hardware.[15] The thinking was that if the software was better, there would be higher demand for the hardware. As a result, software developers had incentives to distribute their source code to universities and lab engineers to improve the software by finding bugs and fixing the source code.[16] However, with the development of a separate software industry in the 1970s and the Personal Computer (PC) revolution, IT solutions started getting unbundled and software programming in itself became a lucrative profession. Microsoft was established in July 1975 as an organization that, almost exclusively, wrote and sold programming language for PCs.[17] It was this transformation of software into a digital monetizable product whose consumption was non-rivalrous that motivated the movement from open source code to closed source code. Making the source code freely available would make a software non-excludable as well- giving it the characteristics of a public good. Locking up the source code meant that it could be leveraged as an IP. Programme developers woke up to the reality that they had a goose that could lay golden eggs- source code.

As a reaction to these developments, appalled by how software companies had started milking their proprietary software and how the corporate hierarchical structure was damaging the quality of software, a community of programmers founded the Free and Open Source Software (FOSS) which led to the establishment of Free Software Foundation (FSF). The FSF assemblage looked at proprietary software as a system that is "based on dividing the public and keeping users helpless."[18] Richard Stallman, the founder of FSF observed in his book "Open Sources" that under the proprietary software system the first step in using a computer was to promise not to help your neighbour. A cooperating community was forbidden. The rule made by the owners of proprietary software was: If you share with your neighbour, you are a pirate. If you want any changes, beg us to make them."[19] FSF created a licensing agreement- General Public License (GPL)- that challenged the foundations of a copyright agreement. Referred to as "copyleft" counter-intuitively, the GPL is an agreement entered into between the creator of a software and its user which allowed the user to

[14] Richard Stallman, "The GNU Project," available online at https://www.gnu.org/gnu/thegnuproject.en.html (accessed on 07.03.2017)

[15] "E-Commerce and Development Report," *United Nations Conference on Trade and Development*, 2003, 99

[16] Ibid 98

[17] "Key events in the history of Microsoft," available at download.microsoft.com/download/7/e/a/7ea5ca8c-4c72-49e9.../keyevents.doc (accessed on 07.03.2017)

[18] Richard Stallman, "The GNU Project," available online at https://www.gnu.org/gnu/thegnuproject.en.html (accessed on 07.03.2017)

[19] Ibid

do more than just consume the software. The user is permitted to run, study, change, modify and distribute the modified the programme but she is prohibited from closing or restricting a software that was co-operatively developed. Often referred to as the "viral clause" of the GPL - it compels anyone releasing software that incorporates copylefted code to use the GPL in their new release. The GNU/Linux operating system, which was the most famous spin off from the FSF movement, was able to capture substantial market share by late 1990s and continues to be a credible competitor of Microsoft. Today, there is a wider range of licensing agreements to choose from- Apache, Berkeley Software Distribution (BSD), Boost, Creative Commons, MIT etc- which are fundamentally similar to the standard GPL terms but had differences with the moralistic position against proprietary software that FSF and GPL had espoused and provides flexibilities to incorporate pieces of proprietary code along with free code. Broadly, OSS licensing arrangements can be classified as permissive licenses- in which the redistributor of the modified software is not mandatorily required to keep the source code open (Apache, MIT and BSD are the most popular permissive licenses) and copy left licenses- in which the publication of source code is mandatory (GPL is a classic example of copy left license).

ADVANTAGE OSS: BRIDGING THE NORTH-SOUTH DIGITAL INEQUITY THROUGH OPEN SOURCE

Opening up the source code creates a platform for collaborative development of the software by creating a thriving ecosystem of beta-testers and co-developers looking critically at stability problems and proposing bug fixes faster than any proprietary software corporation. This was famously captured in 'Linus' Law' formulated by Eric S Raymond which states that "given enough eyeballs, all bugs are shallow".[20] OSS makes it possible to move a software programme from its original operating system to another operating system environment (porting) and customize the software to adapt to different regulatory, cultural and linguistic requirements. This could have considerable development implications as it allows local programmers to tailor the software to meet local regulatory requirements and possibly translate the operating system into local languages. Most importantly, for developing countries OSS provides an incubatory platform that has the potential to

[20] Raymond ES, The cathedral and the bazaar. www.catb.org/~esr/writings/cathedral-bazaar, 2000 (accessed on 07.03.2017)

breed software developers and IT experts, equipped with the cutting edge software coding skills, who are critically important for the emerging knowledge economy.

Proprietary software perpetuates the monopolistic pattern of the software industry and markets by locking the software buyers into using the software as distributed by the controlling monopolist. As the source code remains a zealously guarded secret, users are technologically dependent upon the original developers for upgrades, bug fixes and customization of the software to meet local needs. Monopoly status and technological dependency is further aggravated by the de facto legitimacy that an existing software programme gains through "network effects". This means that the value of a software increases dramatically and disproportionately as it grows and more number of people start using it and as more hardware processors become compatible with that software.[21] Extant players become deeply entrenched in the market even when there are other, possibly better, open source software options. The tragedy of this technology dependency is further heightened by its stark North-South divide. A look at the biggest global software firms in 2017reveals that the top ten firms (on the basis of market capitalisation) are all from the developed North (Table 1). Developing countries continue to remain software takers from the advanced countries and, if these are proprietary softwares, firms and public bodies in developing countries get locked into a vicious circle of purchasing software by making a significant upfront investment on license fees, followed by software and hardware upgrades and changes in data formats that require investing in new license fees and critical retraining. The outflow of foreign exchange can adversely affect the balance of payment situation and take a significant toll on the already squeezed up IT budgets of developing countries.

RANK	ORGANISATION	HEADQUARTERS	MARKET CAPITALIZATION (as of February 2017)
1.	Microsoft	United States	$407 Billion
2.	Oracle	United States	$168.9 Billion
3.	SAP	Germany	$98.4 Billion
4.	Salesforce.com	United States	$51.9 Billion
5.	Adobe Systems	United States	$47.4 Billion

[21]Network effects partially explain the dominating global presence of MS Office Suite (MS Word, MS Excel, MS PowerPoint). Known as Metcalfe's Law, this method of valuation has been used to explain the value of social networks, computer networks and the Internet.

6.	Intuit	United States	$26.3 Billion
7.	VMware	United States	$24.7 Billion
8.	Fiserv	United States	$21.9 Billion
9.	Dassault Systemes	France	$20.2 Billion
10.	Amadeus IT Holdings	Spain	$19.6 Billion

Source: Forbes: The World's Biggest Public Companies, Software/Programming. https://www.forbes.com/global2000/list/#industry:Software%2520%2526%2520Programming (accessed on 07.03.2017)

A software programme does not operate in isolation but forms part of a larger technological environment of Information and Communication Technology (ICT) infrastructure. This technological environment in which a software programme is applied is constantly and rapidly evolving. It is unfeasible for original developers to envision the course that technological developments will take in the ICT ecosystem at the time of developing the software; which means that swift upgrades will have to be rolled out to meet the requirements of the new technology. As hardware processing and wireless communication move generations ahead softwares have to keep apace. The pace of such software up gradation will have to be all the more fast in some developing countries where the extant ICT infrastructure is almost obsolete. Also, the software will have to account for the social and cultural matrix of the applicable country. If the source code is kept open or required to kept open by the government, software up gradation can be carried out indigenously. In the case of proprietary software, the software importing country will have to repetitively pay for services related to the software. The enormous implication for developing countries of such continuing dependency can be understood from a survey conducted by the Gartner Group which reported that the cost of software licenses amounts to only 8 per cent of the total cost of ownership,and the other 92 per cent reflects the costs of installation, maintenance, management, and repairs after failures.[22]

The utility of open source code has long since surpassed the domain of software programming and today finds application in Artificial Intelligence (AI), publishing, biotechnology, financing, risk management and education amongst other fields. The Human Genome Project was enabled by the FOSS open source initiative and ensured that the human genome data remains in the public domain. The applicability of open source in biotechnology research projects arises from an awareness

[22] "E-Commerce and Development Report," *United Nations Conference on Trade and Development*, 2003, 99

amongst the scientific community of the importance of open data and procedures, as replicability is the only guarantor of scientific validity.[23] In the education sector, frustrated by the high costs and depreciating quality of proprietary content, a variety of collaborative projects have spawned across the world. Indira Gandhi National Open University (IGNOU), a distance education university in India, which has enrolled more than 4 million students, uses open source tools to develop content which is then pooled and made available for other users. Public schools in Spain, Russia, Germany, Georgia, Philippines among other countries have switched to Linux operating systems. In 2011, Government of India with the objective of extending technology-enable education in India announced the launch of tablets at Rs 1500 ($22) which were pre-installed with Linux. It enabled teachers and students in the remotest corners of India to join virtual classrooms and benefit from lectures delivered by other teachers around the country. The impressive potential that open source code holds in education sector- to contribute to a "knowledge commons"- has immeasurable development implications for countries. Here, it is important to bear in mind that open source code has course-altering applicability in sectors such as education and biology research which might not be deemed to be "critical infrastructure". This overarching applicability of open source code in development and research initiatives becomes important while looking at the trade disciplines proposed for source code under the Trans-Pacific Partnership Agreement (Section IV below)

It is also documented how open source code platforms can be extremely vital from a cyber-security perspective as security researchers can quickly uncover and eliminate security vulnerabilities and deliberate "backdoors"[24] inserted into critical software.[25] It is important to bear in mind that as we progress towards the "internet of things"- the interconnection via the Internet of computing devices embedded in everyday objects, enabling them to send and receive data- the threat of cyber security is not just limited to critical devices but also daily use devices such as smart phones, ACs, cable modems and routers.

As the breadth of products embedded with software programmes increase, it is equally crucial to maintain access to the source code for regulatory oversight as well. Regulatory authorities need to have access to the underlying source code of a product's operating software to verify the product's conformity with characteristics and qualities specified in the technical specifications for that product.

[23]See *www.oreillynet.com/pub/a/network/2002/04/05/kent.html* and *www.wired.com/news/medtech/0,1286,46154,00.html* for more details

[24]"Backdoors" are applications that allow for backdoor access to computers and other devices. Hackers use these backdoor programmes to gain remote access to the victims network.

[25]Jeremy Malcolm, "TPP threatens Security and Safety by Locking down U.S. Policy on Source Code Audit", *Electronic Frontier Foundation*, December 2015.

For example, regulators might have a reasonable interest in inspecting software on devices that host personal data for flaws that could violate users' privacy. Wireless devices like home alarm systems and wearables could be safer if a third party were able to verify the underlying source code for malware. Connected cars and medical devices are hard to check for safety if the only people with access to the source code are the manufacturers.

Some observers have commented that the entry of the OSS model will have an anti-innovative impact on the software industry. The possibility of such an anti-innovative impact allegedly arises from the reduced profitability which stymies Research and Development (R&D) expenditures in the software industry. However, a vast body of independent research shows an overwhelmingly positive impact of the OSS model on innovation and competition in the software industry.[26] The most important pro-innovative features of OSS development model are based on the huge number of programmers who are motivated to innovate through collaboration and the resultant high level of knowledge diffusion. Bitzer and Schroder found that the move from monopoly to duopoly markets increases the technology level and thus the level of innovation chosen by enterprises. Thus, "OSS entry has a positive impact on firms' willingness to innovate and heightens the overall technological level in the industry."[27] Firms are increasingly showing their willingness to work with OSS developers and increasingly resorting to OSS to create new products and services[28]. It is important to remember that in an OSS environment the degree to which a software tool can be utilized and expanded is limited only by the knowledge, learning and innovative energy of the potential users and not by exclusionary property rights, prices or the power of countries and corporations.

Even though there is overwhelming evidence that OSS spurs innovation and increases the competitiveness of software industry and that access to source code is indispensable for security reasons, regulatory oversight and knowledge diffusion, there has been a steady push to prevent governments from promoting or mandating the use of OSS or requiring the disclosure of source code as a condition of import, distribution, sale or use of software or of products containing software. This is visible in trade disciplines that are contained in FTAs and in discussion on trade-related issues of global e-commerce at the WTO.

---

[26] See, Ravi Sen, "A Strategic Analysis of Competition Between Open Source and Proprietary Software," *Journal of Management Information Systems* Volume 24 no.1, 2007; Nicholas Economides and Evangelos Katsamakas, "Two-Sided Competition of Proprietary vs. Open Source Technology Platforms and the Implications for the Software Industry," *Management Science*, Volume 52 no.7, 2006; W Widenius and N Nyman, "The business of open source software: a primer," *Technology Innovation Management Review*, Volume 1, p8-11, 2014; M Hobday, "Firm-Level Innovation Models: Perspectives on Research in Developed and Developing Countries," *Technology Analysis & Strategic Management*, Volume 17no.2, pp. 121–146, 2005.

[27] Jurgen Bitzer and Phillip J H Schroder, "The Impact of Entry and Competition by Open Source Software on Innovation Activity," *International Business Section Working Paper Series* no 12 of 2005

[28] Fred Simon, The future of Open Source: Speeding Technology Innovation, Black Duck Software, 2014

III. INTERFACE OF SOURCE CODE RULES WITH TRADE RULES

DIGITISATION OF PRODUCTION AND TRADE: IMPLICATIONS IN THE REALM OF RULE-MAKING

The digital revolution has brought systemic re-organisation in the structure and pattern of global trade. Today, business models are increasingly leveraging the digital platform in the production and delivery of goods and services. The advent of digital technology has led to the "servicification" or digitisation of goods and manufacturing value chains. The value of many "goods" are now vested less in the physical components of the product and largely in the digital operating system that is embedded in that product. The CEO of multinational automobile manufacturer Daimler recently commented that traditional car-makers may get reduced to becoming the Foxconn (the China-based iPhone manufacturer) of the car industry, while others own the all-important digital operating systems.[29] Studies on the global supply chains of iPhones and iPads have shown that, although most of the components of these Apple products are manufactured in China, the primary benefits go to the U.S. economy as Apple (based in California, U.S.) continues to capture the largest share of value from the innovations that go into the product's design, software development, product management, marketing and sales.[30]

An important ramification of this pattern of re-organisation is that traditional division of rules on market access based on goods (GATT) and services (GATS) has become nebulous. GATT disciplines will start applying for services to the extent that these services are embedded in goods and vice versa. Rules on source-code will have a strong interface with rules that impinge upon trade in goods (GATT, TBT, SPS), Trade-Related Aspects of Intellectual Property Rights (TRIPS) and trade in services (GATS). It is important that the multilateral discussions examining the trade-related issues of e-commerce proceed in a manner that harmonizes itself with trade rules in related disciplines. The following analysis examines the interface of rules on source-code with the entire gamut of trade rules:

[29] Singh P, "A borderless economy that will be controlled" *The Hindu, http://www.thehindu.com/opinion/columns/a-borderless-economy-that-will-be-controlled/article8581476.ece,* 2016 (accessed on 29 January 2017)

[30] Kenneth L. Kraemer, Greg Linden, and Jason Dedrick, "Capturing Value in Global Networks, Apple's iPad and iPhone", *Personal Computing Industry Centre*, 2011.

1. TRADE RULES ON ANTI-COMPETITIVE PRACTISES

Closing the access to source code can establish the classic conditions for monopoly in software markets and industry. The absolute dependency of the users of the software on developers for the software application, upgrades, bug fixes, maintenance and repair means that the controlling monopolist can charge monopoly prices for each of these services. A company or public institution using proprietary software can get locked in by the controlling software vendor. The vendor enjoys absolute autonomy through "control of the guts of the information systems that are, increasingly the core asset of almost any business".[31]

Prohibiting access to the underlying source code creates a monopoly not only over the software but will also restrict market entry for the repair of electronic products with that embedded software. For example, local car mechanics will not be able to repair the electronic systems of cars if the car manufacturers are not required to give access to the source code of the software. Electronic products with guarded source codes can only be repaired by its manufacturers and authorized repairers. Similarly, protected source codes will also impede markets for innovators who could study these source codes to develop downstream products or diagnostic tools.

It is to be noted that both GATT [*Article II.4*] and GATS [*Article VIII, Article IX*] contain provisions that regulate and discourage anti-competitive practises.

2. TRADE RULES ON TECHNICAL REGULATIONS AND CONFORMITY ASSESSMENT PROCEDURES

The WTO Agreement on Technical Barriers to Trade (TBT Agreement) recognizes the sovereign right of its members to lay down mandatory technical regulations regarding characteristics and related processes and production methods of products. WTO members enjoy the right to lay down technical specifications for software products and products embedded with IT software provided such specifications are not more "trade restrictive than necessary to fulfil legitimate objectives" and are consistent with the provisions contained in GATT and TBT Agreements. US proposal, by placing limitations on the regulatory right to lay down technical specifications such as source code disclosure on software products, goes beyond the WTO framework. The US submission proposes

[31]Steven Weber, "The Political Economy of Open Source," *BRIE Working Paper* 140, E-conomy Projectä Working Paper, 15 June 2000.

that authorities can "obtain access to source code in order to protect health, safety or other legitimate regulatory goals." However, it omits some other 'legitimate objectives' mentioned in the TBT Agreement- such as prevention of deceptive practises, national security and protection of environment. Also, as has been mentioned above, the opening up of source code has important ramifications for the welfare calculus- such as development initiatives in public education and public health. Source code disclosure requirements may not necessarily be related to protecting 'regulatory goals'.

A WTO member also enjoys the right to assure that its imports conform to the characteristics and qualities specified in the technical specifications for that product as long as the procedures to verify this conformity (conformity assessment procedures) are consistent with the rules laid down in the TBT Agreement. In recent years, security vulnerabilities are being reported not just from modems and PCs but also from daily use devices such as smoke alarms, motor vehicles, drink mixers, medical devices etc. It is important to bear in mind that unlike the US proposal at the WTO (which contains an exception that protection of source codes shall not hinder the "ability of authorities to access source code in order to protect health, safety or other legitimate regulatory goals") the TPP provisions have imposed an absolute ban on audit/verification of source code by regulatory authorities other than for devices that are used in critical infrastructure and those that are not meant for mass markets. Similarly, TiSA also has no exceptions allowing regulatory authorities to access source codes. Regulatory authorities need to have full access to the source code of softwares embedded in electronic devices to ensure that these devices do not pose a threat to national security and conform to technical specifications on human health or safety, animal or plant life or health or the environment.

3. TRADE SECRETS

US submission to the WTO (JOB/GC/94) proposes that "companies do not have to share source code, trade secrets, […] in order to access new markets […]"..The US government has repetitively expressed concerns regarding the trade-secret regimes around the world and pushed for dedicated domestic legislations on trade secrets in China and India in its most recent National Trade Estimates Report of 2016[32]. Its concerns relate to the difficulty in obtaining damages and the lack of sufficient

[32] National Trade Estimates on Foreign Trade Barriers, *Office of the United States Trade Representative,* available at https://ustr.gov/about-us/policy-offices/press-office/reports-and-publications/2016/2016-national-trade-estimate, 2016.

procedural safeguards to protect against disclosure of trade secrets and other confidential information in civil or criminal litigation. From the language of this US proposal (JOB/GC/94) it seems clear that protection of trade secrets, source code being one amongst them, is at the centre of its agenda. This indicates an attempt to introduce, through the backdoor, TRIPS-plus provisions into the WTO. TRIPS allows member states the policy flexibility to deal with trade secrets. *Article 39* of the TRIPS Agreement sets out minimum levels of protection for undisclosed information[33] and very few WTO members have dedicated national legislations to protect and enforce rights over trade secrets. The divergence in domestic practises in addressing the scope and meaning of and level of protection for trade secrets was also emphasised in a 2014 Report of the OECD titled "Approaches to protection of undisclosed information (Trade Secrets) in 11 OECD countries and the BRICS countries".[34]

4. INDIGENOUS TECHNOLOGY

The US paper also proposes that "It is important to ensure that companies do not have to share source code, trade secrets, or substitute local technology into their products and services in order to access new markets [...]".

Currently under the WTO framework, members have the policy flexibility to require local sourcing of technology as a market-access condition for trade in service industries as long as they are included in a country's schedule of commitments under the General Agreement on Trade in Services (GATS), either in specific sectors or horizontally depending on their nature. Since GATS follows a positive list approach, the obligation to list the local sourcing requirements extends only to those sectors which the member had voluntarily agreed to take up commitments. The requirement in the US proposal that WTO members should be prohibited from imposing local sourcing of technology in services as a market access condition goes beyond the GATS mandate, thereby prejudicing the development and use of indigenous technology.

5. TECHNOLOGY TRANSFER

[33] *Article 39.2* provides that natural and legal persons shall have the possibility of preventing information lawfully within their control from being disclosed to, acquired or used by others without their consent in a manner contrary to honest commercial practises.

[34] The paper is available at:
http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=TAD/TC/WP(2013)21/FINAL&docLanguage=En

Considering that, in digital products, source code constitutes an integral component of the technology, WTO proposals seeking to prohibit the transfer of source code effectively prohibits the transfer of technology from a foreign investor to a local company. It is to be noted that the WTO Agreement on Trade-Related Investment Measures (TRIMS Agreement) allows member countries the flexibility to require technology transfer in case of foreign investment. To that extent, the proposals on source code contains a TRIMS-plus element.

IV. FTA DISCIPLINES ON ACCESS TO SOURCE CODE

RULE MAKING ON SOURCE CODE IN FTAS

Most of the elements contained in this proposal on source-code trace their origins to provisions contained in US-led regional/plurilateral trade coalitions such as the Trans-Pacific Partnership (TPP) and the Trade in Services Agreement (TiSA). ***Article 14.17*** **of the TPP** provides:

1. *No Party shall require the transfer of, or access to, source code of software owned by a person of another Party, as a condition for the import, distribution, sale or use of such software, or of products containing such software, in its territory.*
2. *For the purpose of this Article, software subject to paragraph 1 is limited to mass-market software or products containing such software and does not include software used for critical infrastructure.*
3. *Nothing in this Article shall preclude:*
    a. *the inclusion or implementation of terms and conditions related to the provision of source code in commercially negotiated contracts; or*
    b. *a Party from requiring the modification of source code of software necessary for that software to comply with laws or regulations which are not inconsistent with this Agreement*
4. *This Article shall not be construed to affect requirements that relate to patent applications or granted patents, including any orders made by a judicial authority in relation to patent disputes, subject to safeguards against unauthorized disclosure under the law or practise of a Party.*

There is very little clarity as to the scope, potential implications and the inter-linkages of this provision with e-commerce disciplines. An examination of similar provisions in other FTAs suggests

that the disciplines on source code might have been originally conceived by Japan. A leaked text of the Trade in Services Agreement (TiSA) (February 20, 2015) contains a provision on source code that was proposed by Japan and opposed only Colombia. Strikingly, the language proposed by Japan for TiSA is far more restrictive than Article 14.17 of TPP as the former contains lesser exceptions. Article 6 of the leaked version of the TiSA contains the following proposal under the title "Transfer or Access to Source Code":

No Party may require the transfer of, or access to, source code of software owned by a person of another Party, as a condition of providing services related to such software in its territory.

Disciplines curtailing governments from requiring access to source code are also present in the Japan-Mongolia FTA which was concluded in 2010 and came into force in 2016. ***Article 9.11*** **of the Japan- Mongolia EPA** contains provisions on source code that resembles the TiSA language very closely:

> *Neither Party shall require the transfer of, or access to, source code of software owned by a person of the other Party, as a condition of the import, distribution, sale or use of such software or of products containing such software in its Area.*

The genesis of such disciplines can perhaps be attributed to concerns regarding source code disclosure requirements as market-access criteria particularly in China. Towards the end of 2014, China issued *Circular No.317* (Guidelines on Promoting the Application of Secure and Controllable IT, Year 2014-2015) which requires companies selling computer equipment to Chinese banks to disclose their source code and submit their equipments for internal audits. Other than the pursuit of legitimate regulatory and policy objectives (protecting cyber security, preventing deceptive practises, conformity of products with domestic technical standards for IT and IT enabled products) there could be obvious political economy considerations of, *inter alia,* incentivising indigenous innovation or curtailing the outflow of foreign exchange in the form of license fees for proprietary software, behind requiring the transfer of or access to the source code in proprietary software. Disciplines seeking to prohibit source code disclosure could freeze the policy flexibility that is hitherto available for governments to pursue such regulatory objectives and development goals. More importantly, extant FTA disciplines prohibiting governments from requiring transfer of or access to source code could seriously inhibit the use or promotion of open source softwares. All the FTAs envisage a broad prohibition by using the terms "transfer of or access to" source code. Although no definitions

of these terms are available within the text of the FTA, an ordinary interpretation of these terms within their context suggests the following:

1. "Transfer of source code" will prohibit FTA parties from requiring foreign investors to transfer source code to a local company.
2. "Access to source code" will have implications for government regulators seeking to audit the source code for conformity with domestic laws on security, deceptive practises etc.

Strikingly, the TPP text in *Article 14.17* also uses the term "disclosure of source code" which seems to be directed towards prohibiting the requirement to disclose the source code to the general public by publishing it online.

The next section discusses the implications of FTA provisions on source code for developing countries.

IMPLICATIONS OF FTA PROVISIONS FOR DEVELOPING COUNTRIES

1. IMPACT ON PUBLIC PROCUREMENT POLICIES

Governments, in both developing and developed countries have instituted policies mandating the use of or providing preferential treatment to open source software (Part V below highlights some of such policies maintained by governments and brings out how extensively OSS is used in public institutions). The prohibition contained in Article 14.17 of TPP- that no party shall require the access to source code as a market access condition for such software- had given rise to the concern that it may limit the ability of governments to institute such public procurement policies. However, a carve out for "government procurement" in Article 14.2.3 of the e-commerce chapter in TPP allays these fears; unfortunately only to some extent. Ambiguously crafted provisions contained in the TPP could still potentially obstruct a TPP signatory government from instituting or maintaining government procurement policies that mandate the use of or accord preferential treatment to OSS.

Firstly, the Intellectual Property (IP) rights chapter of TPP contains disciplines that regulate "Government Use of Software". ***Article 18.80*** **Para 2** provides the following:

> 2. *Each Party shall adopt or maintain appropriate laws, regulations, policies, orders, government-issued guidelines, or administrative or executive decrees that provide that its* ***central***

> ***government agencies use only non-infringing computer software protected by copyright and related rights****, and, if applicably only use that computer software in a manner authorised by the relevant license. These measures shall apply to the acquisition and management of the software for government use.*[35] (emphasis supplied)

A paper published by Open Source Industry Australia highlights that such a provision, by requiring central government agencies to use only non-infringing computer software protected by copyright and related rights, could prohibit central government agencies of signatory governments from using any software that is in the public domain[36]. Indeed, all open source softwares do not fall within the realm of public domain. OSS usually operates on the basis of a license where the author retains certain rights[37] over the software and the license allows the author to enforce these rights if they are violated. For example, when a software is licensed under GPL, the license can be used by the author, for instance, to enforce the copyleft clause contained in the GPL license. A public domain software cannot have a license which would impose terms on its users or grant rights to its authors akin to that of an open source license. It refers to software that is explicitly placed in the public domain by its author. Richard Hipp, founder of SQLite (a public domain software), believes that public domain software is a subset of OSS.[38] A significant number of programme developers continue to place their software directly on the public domain. Some of the most widely used and indispensable computing tools such as Berkeley yacc (a compiler generator), SQ Lite (a relational database management system that is embedded in end programmes like Adobe Systems, Evernote, Skype) are public domain software. These are tools that are profusely used in computing research and development facilities. TPP effectively prohibits research labs and universities of the central government from using such softwares or using programmes that have such softwares embedded within them. *Article 18.80* would also apply to softwares that are kept under the public domain through Creative Commons Zero (CC0) License. A software that is licensed under CC0 allows the author to relinquish to waive all her copyright and related rights in her works, effectively placing it in the

---

[35] For greater certainty, paragraph 2 should not be interpreted as encouraging regional government agencies to use infringing computer software or, if applicable, to use computer software in a manner which is not authorized by the relevant license. (citation in original text)

[36] "TPP prohibits government use of public domain software," Submission to the Commonwealth Joint Standing Committee on Treaties regarding the Trans-Pacific Partnership, Open Source Industry Australia Limited, p15, 11 March 2016.

[37] Whether such rights, as are guaranteed under the license agreements of open source softwares, fall within the normative definition of "copyright and related rights" can itself be contested and is open to legal interpretation. If one is to take the position that the rights guaranteed by OSS license arrangements do not fall within the domain of copyrights, then this could effectively prohibit governments from using the entire range of OSS software.

[38] Stephen Shankland, "Is Public Domain Software Open Source?," CNet, available at https://www.cnet.com/news/is-public-domain-software-open-source/

public domain.[39] Notably, Europeana, Europe's meta-aggregator and display space for digitised works of music, art, etc releases its metadata into the public domain using CC0. It is to be noted that *Article 18.80* constitutes a TRIPS-plus obligation on TPP parties as the TRIPS Agreement contains no obligations stipulating central government agencies to procure only non-infringing software protected by copyright and related rights.

Secondly, ***Article 14.4*** contained in the e-commerce chapter of TPP mandates "non-discriminatory treatment of digital products". It provides:

> 1. *No Party shall accord less favourable treatment to digital products created, produced, published, contracted for, commissioned or first made available on commercial terms in the territory of another Party, or to digital products of which the author, performer, producer, developer or owner is a person of another Party, than it accords to other like digital products.*[40]

As has been mentioned earlier, several governments maintain public procurement policies that mandate the use/purchase of or accord preferential treatment to open source softwares and thereby discriminate against proprietary software for a variety of reasons- security issues and avoidance of vendor-lock in situations not the least among them. The flexibility of governments that are signatory to TPP to discriminate against proprietary software through such policy initiatives will depend on the legal interpretation of whether proprietary software and open source software are "like digital products".

On the other hand, TiSA or the Japan-Mongolia FTA has no exceptions for government procurement as is contained in the TPP. Signatory governments to these FTAs are, or likely to be, prohibited from requiring the disclosure of software source codes of products that are procured by governmental agencies or mandating the openness of a source code as a requirement to participate in public procurement. Countries, particularly developing countries stand to benefit from an OSS model (as noted above) and should at least have the choice to promote OSS if they feel that it is worth promoting and provides better security, reliability and/or cost-effectiveness when compared to proprietary software. In particular, developing countries would want that specific solutions remain open source, because of legitimate public policy reasons such as opening the maintenance and

[39]"No Rights Reserved," *Creative Commons*, available at https://creativecommons.org/share-your-work/public-domain/cc0/

[40] For greater certainty, to the extent that a digital product of a non-Party is a "like digital product", it will qualify as an "other digital product" for the purposes of this paragraph. (citation in original)

support market avoiding vendor lock situations (where the maintenance and support systems of a run are monopolized by the vendor) or ensuring better transparency through code transparency.[41]

2. IMPACT ON OPEN SOURCE LICENSING

Paragraph 1 of *Article 14.17* prohibits a *Party* to the TPP from requiring the transfer of, or access to software source codes as a condition for being imported into or sold or used on that State's territory. Relevant definition of "Party" is contained in *Article 1.3* of the TPP Agreement and refers to: "any State or separate customs territory for which this Agreement is in force." A plain reading of this provision suggests that it prohibits only signatory governments from requiring source code disclosures as a market access conditionality and does not prohibit open source licensing between private parties. Paragraph 3 further narrows the scope of the prohibition by exempting "commercially negotiated contracts" from its ambit. It provides that "Nothing in this Article shall preclude the inclusion or implementation of terms and conditions related to the provision of source code in commercially negotiated contracts". Open source licensing arrangements which contain terms requiring the source code to be transferred or kept open will be permitted if these arrangements are commercially negotiated.

However, a more nuanced analysis of *Article 14* suggests that the provision will have ramifications for licensing arrangements between private parties as well. To begin with not all software licenses in the open source licensing domain are "commercially negotiated" and, therefore, will not attract the exception of *Paragraph 3 (a)*. GNU General Public Licenses, which are arguably the most popular software licenses in this domain are not "commercially negotiated". Imagine a scenario where the licensee of a GPL- licensed OSS violates the copyleft terms of the license and converts the OSS into proprietary software. The government or the judicial authority of a TPP signatory Party will be proscribed from enforcing the terms and conditions of such a non-commercially negotiated contract.[42] What is notable is the omission of the word "enforcement" from the phrase "inclusion or

[41]Jason Williams, Peter Clegg, Emmett Dulaney, "The advantages of adopting Open Source Software," InformIT, May 6,2005 available at http://www.informit.com/articles/article.aspx?p=376255&seqNum=8, (accessed on 09-03-2017)

[42] Sub para 4 of Article 14.17 has a very specific carve out that the Article shall not apply to "orders made by a judicial authority in relation to patent disputes." Kilic and Israel commented that it is concerning that the protection is only available for patent disputes and not made available for other types of legal disputes where access to source codes might be equally necessary. See, Burcu Kilic and Tamir Israel, "The Highlights of the Trans-Pacific Partnership E-commerce Chapter," *Public Citizen* and *Canadian Internet Policy and Public Interest Clinic*, November 2015

implementation". This means that even in cases of breach of licenses which are commercially negotiated, the remedy of specific performance (where the licensor seeks to enforce the terms requiring transfer of or access to source code) might not be available to the licensor of the OSS.

An article published by Software Freedom Law Centre (SFLC) rules out the possibility of *Article 14.17* having any implications for free software, open source licensing arrangements between private parties, governmental acquisition of OSS.[43] It reaches this conclusion by looking at the context- the mischief that the rule intends to remedy (Japan's concerns on mandatory disclosure of source code for accessing Chinese markets), the placement of the rule in e-commerce chapter and not in the chapter on IP, exceptions to the rule which further narrows down its applicability and most pivotally the use of the term "Parties" in *Article 14.17*. However, this conclusion can be questioned on at least three grounds. Firstly, established jurisprudence on trade disputes constitute a poignant reminder of how the initial mischief that a law sets out to remedy often has no direct connection with the final shape such law evolves through legal interpretation. This is to say that, although *Article 14.17* might have taken birth to address Japanese market access concerns that does not ipso facto prevent the application of this rule to other areas of source code litigation. Secondly, SFLC's article offers no argument as to why *Article 14.17* will not interfere with the enforcement of open source licensing arrangements. In disputes, such as those involving the violation of a copy left license between private parties, *Article 14.17* will prohibit TPP parties from enforcing specific performance by requiring the source code to be kept open by the licensee. Thirdly, as explained above, *Article 18.80*, read along with *Article 14.2.5 (b)*[44] of TPP, will prohibit governments from giving preference to non-copyrighted software such as public domain software in government procurement.

3. THREAT TO SAFETY AND SECURITY

The prohibition on source code disclosures do not extend to bespoke applications (applications that are not for "mass market") and "critical infrastructure". However the TPP text does not define either of these terms and the precise scope of these exemptions remain unclear. As has already been noted, security vulnerabilities arising from malicious software, snooping on personal information

[43] "TPP Article 14.17 & Free Software: No Harm, No Foul," *Software Freedom Law Centre*, available at https://www.softwarefreedom.org/blog/2015/nov/23/TPP-Article-14/, November 2015

[44] *Article 14.2.5 (b)* of TPP provides that, *Article 14.17* (Source code) is "to be read in conjunction with any other relevant provisions in this Agreement."

and deliberate backdoors are not just limited to "critical infrastructure"- however broadly such a term gets defined- but extends to daily use devices[45], medical devices[46] etc.

On the other hand, the requirement to disclose software source codes in the case of critical infrastructure can potentially cause invasion of privacy or censoring network activities. Tamir Israel, writing in the context of similar exception contained in the TiSA observes that "there could be good reasons to prevent a particular government from accessing source code for software used in critical infrastructure. To give just one example, a regulator may wish to impose audit obligations in order to check the filtering or monitoring capacities of Deep Packet Inspection equipment (an advanced method of packet filtering that examines data contained in a packet as it passes through an inspection point) installed in a mobile or wire line service provider's network."[47]

The exceptions contained in TPP text on source code transfer obligations are counter-productive, ill-nuanced and does not protect from security vulnerabilities or curtail regulatory overreach by way of breach of privacy or censorship. It is both overarching and undermining at the same time.

4. IMPACT ON CONFORMITY ASSESSMENT PROCEDURES

In 2015, the Environmental Protection Agency (EPA) of the United States found out that the German automobile manufacturer Volkswagen had intentionally pre-programmed the software in its turbocharged direct injection (TDI) diesel engines to activate certain emission controls only during laboratory emissions tests. The actual on-road emissions by the same Volkswagen engines were found to be 40 times higher than the emissions allowed under the US Clean Air Act. From the findings of EPA it was also clear that Volkswagen was able to maintain this test-subverting software for seven years because the regulators had no access to the embedded computers of the automobile.[48]

---

[45] Catalin Cimpanu, "RSI Videofied Security Alarm Protocol Flawed, Attackers Can Intercept Alarms," *Softpedia*, November 30, 2015; Catalin Cimpanu, Vulnerabilities in 8 Modems Could Lead to the Creation of a WorldWide Botnet," *Softpedia*, December, 2015

[46]Vulnerability Note VU#630239, "Epiphany Cardio Server is vulnerable to SQL and LDAP injection," *Vulnerability Notes Database*, Homeland Security, US, 2015

[47] Tamir Israel, "TiSA Annex on Electronic Commerce: A Preliminary Analysis," *Canadian Internet Policy and Public Interest Clinic*,

[48] Klint Finley, "Trade Pact Could Bar Governments From Auditing Source Code", *Wired*, Novermber 5 2015.

Zeynep Tufecki, writing in the aftermath of the Volkswagen scandal, observed the following: "In a world where more and more objects are run by software, we need to have better ways to catch such cheaters. As the Volkswagen case demonstrates, a smart object can lie and cheat. It can tell when it's being tested, and it can beat the test. [..]If precautions are not extended to the emergent realm of computer-enhanced objects, especially when the software is proprietary and thus completely controlled by the corporation that has huge incentives to exaggerate performance or hide faults during tests for regulatory benchmarks, Volkswagen will be neither the first nor the last scandal of the Internet of Cheating Things."[49] The ubiquitous use of such "defeat devices" in softwares is what has made cyber experts propose the idea that, manufacturers of WiFi routers, gambling machines and voting machines should release the code that runs these devices to regulators.[50]

Members to the WTO enjoy the right to set technical specifications for products to prevent such deceptive practises, protect human health and safety, animal and plant life and health, environment and other legitimate objectives. They also have the right to ensure that the imported products are in conformity with such technical specifications as long as these technical specification and conformity assessment procedures are in conformity with the TBT Agreement. *Article 14.7* of the TPP effectively shuts the door for regulators in TPP countries to require companies to hand over their source code to verify their conformity with technical regulations preventing deceptive practises and other legitimate public policy goals. The exception contained in *Paragraph 3(b)* only provides for Parties to require the modification of source code so as to ensure compliance with laws or regulations. It remains unclear how Parties will determine the compliance of source codes with their laws or regulations when they do not have access to the said source code.

[49] Zeynep Tufekci, "Volkswagen and the Era of Cheating Software," *The New York Times*, September 23, 2015
[50] Darlene Storm, "Vint Cerf and 260 experts give FCC a plan to secure WiFi Routers," Computer World, October 2015

V. OPEN SOURCE POLICY INITIATIVES IN SELECT COUNTRIES

Legislations and policies requiring the disclosure of source code are in force in several developing countries. Analysis of these provisions will help in better understanding the objectives (security, stimulating indigenous innovation, conformity assessment, levelling the playing field by disrupting monopolies etc) behind seeking the disclosure of source code. The proposal to develop global rules to prohibit or regulate the disclosure of source code is underpinned by the pressure exerted by commercial interests and lobby groups situated in advanced countries that seek unconditional market access for their technologies and technology-embedded products. A perusal of the submissions made by commercial groupings that represent the established software industry in US such Business Software Alliance (BSA) and International Intellectual Property Alliance (IIPA), to the US Trade Representative (USTR) on whether US trading partners should be designated as Priority Foreign Country, Priority Watch List or Watch List in the 2015 Special 301 Report provides telling evidence regarding the genesis of TPP provisions on source code.

CHINA

In early 2015, the Cyberspace Administration of China (CAC) announced that it had finalized a draft of the National Cybersecurity Review Regime (NCRR), which is expected to be submitted to the Office of the Central Leading Small Group for Cybersecurity and Informatization for review. Although the details regarding NCRR remain nebulous, indications suggest that it contains requirements to disclose source code or turn over encryption algorithms and solutions.[51] The submission made by BSA to USTR in 2015 had flagged concerns regarding turning over source code for security purposes and alleged that only local companies will stand to qualify if such requirements are imposed.

In 2014, China issued *Circular No.317* (Guidelines on Promoting the Application of Secure and Controllable IT, Year 2014-2015) which requires companies selling computer equipment to Chinese banks to disclose their source code and submit their equipments for internal audits. Much earlier than that, close on the heels of the Snowden revelations the Chinese Communist Party had unveiled the "*Decision on Some Major Issues Concerning Comprehensively Deepening the Reform*" which is the CPC's

[51] "New Rules in China Upset Western Tech Companies," *New York Times*, https://www.nytimes.com/2015/01/29/technology/in-china-new-cybersecurity-rules-perturb-western-tech-companies.html?_r=0

policy framework on cyber security. That cyber security lies at the cynosure of China's policy objectives was better understood when the Cyberspace Administration of China was constituted in 2014 with the Chinese President and Premier as its leader and deputy leader respectively. Earlier to this was launched, what is today popularly dubbed, the "De-IOE movement" spearheaded by Wang Jian, Alibaba group leader to replace the strong hold of the tripartite software powerhouses- IBM, Oracle and EMC Corp (hence the acronym "IOE") in China over e-commerce vendors and financial institutions. Wang Jian decided that Alibaba will use X86-based PC servers running on the open-source Linux operating system. Such a system was found to be several times cheaper because it does away with a mainframe server by linking up several PCs with X86 microprocessors inside which can be linked to each other like a chain to function as a server and thereby replacing a mainframe server. The e-commerce company also built a database management-system of its own with an open-source structure, and started storing data on an internal cloud-storage system just like Amazon and Facebook. By May 2013, Alibaba had already pulled the last plug on the IBM server and by July 2013 its advertising systems stopped using the Oracle server. Financial institutions in China are currently emulating the model of Alibaba with some policy nudges from the government like the Circular No.317. Sales and revenue of US-based IT giants such as IBM, Oracle and Cisco from China have plummeted drastically since 2008 forcing them to petition the US government. The story of Alibaba is perhaps an apt illustration of how use of open source softwares and reduced dependence on foreign IT systems have helped a company make it's mark on the global e-commerce market.

BRAZIL

Brazil has been gradually, but consistently moving towards the use of open source software on various platforms since 2003. Since 2003, the Information Technology Institute (ITI) established by the Brazil government has been setting the guidelines, objectives and priority actions for the implementation of OSS within the Brazilian government. In 2007, Rogerio Santanna, Secretary, Secretary of Logistics and IT at the Brazilian Ministry of Planning, Budget and Management observed that open source "reduces costs, increases the competition, creates jobs and develops the knowledge and intelligence of our country. Our preference for open source is not motivated only by economic aspects. But there is also the possibility to develop new products, distribute the

knowledge, access to new technologies and to stimulate the development of software in collaborative environments."[52]

On May 5 2014, the Brazilian Government published an Inter-Ministerial Ordinance (141/2014) that requires all IT equipment sold to government institutions and public enterprises to be certified to be clear of security threats and backdoors. For meeting the requirements of the certification system there must be the possibility of auditing programs and equipment which, in turn, requires the possibility of "opening the source code in the case of programs for data communication and firmware and operating systems in the case of data communication equipment".[53]

Ordinance 141/2014 is itself based on Decree 8135/2013 which includes requirements to calls for auditing of hardware and software used in government data communications.

In its submission to the USTR for the Special 301 Report, BSA flags concerns regarding Decree 8135/2013:

"The draft regulations (Decree 8135/2013) present multiple serious problems for BSA members, especially deviation from global standards and requirements to disclose or register source code and other intellectual property. BSA appreciates the opportunity provided by the Ministry of Planning to contribute input via public written comments, which we submitted in late 2014, and through subsequent meetings to be held in late February 2015. BSA hopes that, as a result of this dialogue, the Brazilian government will implement measures that effectively enhance the cybersecurity of government agencies without imposing unnecessary market access barriers to BSA member products and services."[54]

RUSSIA

In 2007, the Russian Ministry of Communications mandated that by 2009 all schools in Russia install domestically developed Linux open source software for their computers to reduce Russia's dependence on foreign proprietary software.[55] In 2008, the Government of Russia and Cuba signed an agreement to collaborate on research and development of open source software. In 2010, Dmitry

[52] The full report is available at http://www.softwarelivre.gov.br/publicacoes/DTA_ITI.pdf
[53] Interministerial Ordinance MP / MC / MD Nº 141 of 05/02/2014, Chapter V, Article 14. The text is available at https://www.legisweb.com.br/legislacao/?id=269793
[54] Business Software Alliance, Special 301 Submission, 2015, available at http://www.bsa.org/~/media/Files/Policy/Trade/BSA2015Special301.pdf
[55] "Russian Schools move to Linux," *BBC,* 2007, available at http://news.bbc.co.uk/2/hi/technology/7034828.stm

Medvedev introduced amendments to the Russian Civil code to incorporate and give legal status to open source licensing.

SOUTH AFRICA

In 2006, the Department of Public Service and Administration of South Africa adopted the "Policy on Free and Open Source Software Use for South African Government"[56] which provides that:

1. The South African Government will implement FOSS unless proprietary software is demonstrated to be significantly superior. Whenever the advantages of FOSS and proprietary software are comparable FOSS will be implemented when choosing a software solution for a new project. Whenever FOSS is not implemented, then reasons must be provided in order to justify the implementation of proprietary software.
2. The South African Government will migrate current proprietary software to FOSS whenever comparable software exists.
3. All new software developed for or by the South African Government will be based on open standards, adherent to FOSS principles, and licensed using a FOSS license where possible.
4. The South African Government will ensure all Government content and content developed using Government resources is made Open Content, unless analysis on specific content shows that proprietary licensing or confidentiality is substantially beneficial.
5. The South African Government will encourage the use of Open Content and Open Standards within South Africa.

INDIA

In 2012, Government of India launched the National Policy on Information Technology which identifies adopting open standards and promoting open source and open technologies as one of the thrust areas of the policy.[57]

In furtherance of the need to set up hardware and software infrastructure as part of the Digital India Programme of the Government of India formulated the "Policy on Adoption of Open Source Software for Government of India"[58] in 2013 to adopt OSS in all e-Governance systems

[56] Full text available at http://www.gov.za/sites/www.gov.za/files/foss_policy_0.pdf

[57] "National Policy on Information Technology 2012", *Ministry of Communications and Information Technology*, Government of India, available at http://pib.nic.in/newsite/PrintRelease.aspx?relid=87875

[58] F. No. 1(3)/2014 – EG II, *Ministry of Communication & Information Technology Department of Electronics & Information Technology*, Government of India, available at

implemented by various Government organizations, as a preferred option in comparison to proprietary software. It mandates governments to include a specific requirement in the request for proposal for all suppliers to consider OSS along with proprietary software while responding to the request. Suppliers have to provide justification for exclusion of OSS in their response, as the case may be. Government Organizations shall make their decision on the suitable software by comparing both OSS and proprietary software options "with respect to capability, strategic control, scalability, security, life-time costs and support requirements."

The policy will have applicability to all government organisations under the Central and State governments that choose to adopt this policy for Anew e-governance applications and new versions of existing systems.

NIGERIA

In 2014, the Nigerian government released the Guidelines for Nigerian Content Development in Information and Communications Technology. According to these guidelines Ministries, Departments and Agencies of government at the Federal, State and Local levels are "required to obtain evidence of the origin, source and workings of all software being used including adequate assurance of the full security of source code."[59] *Guideline 11.3* (Guidelines for Indigenous Software Development) provides that "multi-national companies shall provide verifiable information and sign affidavits about the origin, safety, source and workings of software being sold and deployed within the country in order to ascertain the full security of the product and protect national security." *Guideline 11.4* provides that all Ministries, Departments and Agencies of government at all three tiers, Federal, State and Local, as well as in all three branches, Executive, Legislative, and Judiciary "shall source and procure software from only local and indigenous software development companies; where the capacity for developing such software does not exist locally, procurement, installation and support will be provided by a Nigerian company".

The BSA's country report on Nigeria for 2015 had some scathing criticism for the Nigerian Guidelines:

---

http://meity.gov.in/sites/upload_files/dit/files/policy_on_adoption_of_oss.pdf

[59] "Guidelines for Nigerian Content Development in Information and Communication Technology," *Office for Nigerian Content Development in Information & Communication Technology,* available at http://onc.org.ng/wp-content/uploads/2014/06/ONC-Framework-2.pdf, 2014

"If these guidelines are implemented, Nigeria would become one of the most restricted and closed ICT markets in the world. Specifically, the Guidelines impose stringent local content requirements for ICT hardware, software, and services for government and private sector procurements, restrict employment of non-Nigerian citizens in the sector, force technology transfer, require the disclosure of source code and other sensitive design elements as a condition of doing business, and impose severe data and server localization requirements."[60]

INDONESIA

In 2009, the Ministry of Administrative Reforms of the Government of Indonesia issued Circular No.1 of 2009 on "Utilization of Legal Software and Open Source Software (OSS)" which endorsed the use and adoption of open source software within government organizations with a view toward implementation by the end of 2011, which will result in the use of legitimate open source and FOSS software and a reduction in overall costs of software.

The International Intellectual Property Alliance (IIPA), an umbrella group for software industry, reacted to the Indonesian Government's circular by alleging that such a policy will weaken the software industry and equates OSS with piracy: Quoting from the IIPA's submission to the USTR:

"[T]he Indonesian government's policy as indicated in the circular letter [...] simply weakens the software industry and undermines its long-term competitiveness by creating an artificial preference for companies offering open source software and related services, even as it denies many legitimate companies access to the government market. Rather than fostering a system that will allow users to benefit from the best solution available in the market, irrespective of the development model, it encourages a mindset that does not give due consideration to the value to intellectual creations. As such, it fails to build respect for intellectual property rights and also limits the ability of government or public-sector customers (e.g., State-owned enterprise) to choose the best solutions to meet the needs of their organizations and the Indonesian people. It also amounts to a significant market access barrier for the software industry."[61]

[60] Business Software Alliance, Special 301 Submission, 2015, available at http://www.bsa.org/~/media/Files/Policy/Trade/BSA2015Special301.pdf

[61] International Intellectual Property Alliance Special 301 Report on Copyright Protection and Enforcement, Indonesia Country Report, 2010, available at http://www.iipawebsite.com/rbc/2010/2010SPEC301INDONESIA.pdf

VI. CONCLUSION

Submissions made by WTO members as part of the WTO Work Programme on E-commerce aim to lock up source code- the magic formula of software- in the digital fortresses of established software players. By prohibiting the access to or transfer and disclosure of source code, the attempt is, unequivocally, to discourage the diffusion of software technology, to perpetuate the technology dependency of developing countries and deepen the digital inequities by further entrenching already established players in developing countries' markets. It is also aimed at minimizing the regulatory control of governments over software security and authenticity.

Almost furtively, these proposals chip away at the policy flexibilities that are hitherto available to the members under extant WTO rules. It strengthens the scope of IP protection available to the owner of trade secrets beyond what is available under *Article 39* of the TRIPS regime. Although, WTO members enjoy the policy flexibility to require transfer of technology in cases of foreign investment under the current TRIMS regime, the source code proposal would effectively prohibit transfer of technology (source code being the technology element of software) from a foreign investor to a local company. If the suggested proposals bear fruition, government regulators will not be able to require access to the source code of a digital device for the purpose of assessing its conformity with domestic technical regulations in pursuance of legitimate objectives like security, prevention of deceptive practises and environmental safety.

Binding obligations that proscribe Parties from requiring source code disclosure, access or transfer are also contained in FTAs such as the TPP. The policy implications for developing countries could be severe if disciplines contained in the TPP, serve as a template for multilateral rules on source code. It is to be noted that the existing domestic measures in many developing countries are not in conformity with TPP rules on source code. Most developing countries are still evolving their ICT strategies and are keen on making them relevant for their development processes. TPP rules, with its overarching scope, ambiguous terms that leave room for mischievous legal interpretations and narrow carve-outs, could practically prohibit the pursuit of legitimate regulatory and development objectives by governments. It portends to hinder the realisation of political economy considerations such as incentivising indigenous innovation or curtailing the outflow of foreign exchange in the form of license fees for proprietary software and could seriously inhibit the use or promotion of open source software.

Under the garb of protecting software source code, the rules on e-commerce would protect incomes of owners of proprietary software while eroding the policy space of countries to pursue developmental priorities and regulatory objectives. Overall, the following are the points of concern that the TPP rules on source code raises:

1. It will create and perpetuate monopolies in the software industry and markets by locking the buyers into using proprietary software thereby stifling competition. It will perpetuate the technology dependency of the software users upon the original developers for upgrades, bug fixes and customization of the software to meet local needs.
2. It ensures a continuous and sustained flow of payments to the developers of proprietary software for updates and maintenance and also for repairs of goods containing proprietary software.
3. TPP rules restrict the use of, or preferential treatment towards, Open Source Software by governments and ensure that proprietary software does not face competition.
4. By prohibiting governments from giving preference to OSS, TPP rules prejudice the policy space available to governments to spur the growth of indigenous software development companies.
5. TPP rules, by prohibiting regulatory authorities from accessing the source code of software, will curtail the policy flexibility that is required to pursue regulatory objectives such as national security, assessing the conformity of products with domestic regulations, prevention of deceptive practices and ensuring consumer safety.

Consequently, if multilateral trade rules on source code use TPP rules as a template it could raise similar serious challenges to the members of WTO, especially those members that are desirous of making their ICT strategies relevant for their welfare calculus and safeguarding their regulatory policy space.

References

1. Burcu Kilic and Tamir Israel, "The Highlights of the Trans-Pacific Partnership E-commerce Chapter," *Public Citizen* and *Canadian Internet Policy and Public Interest Clinic*, November 2015.
2. Catalin Cimpanu, "RSI Videofied Security Alarm Protocol Flawed, Attackers Can Intercept Alarms," *Softpedia*, November 30, 2015; Catalin Cimpanu, Vulnerabilities in 8 Modems Could Lead to the Creation of a WorldWide Botnet," *Softpedia*, December, 2015.
3. Darlene Storm, "Vint Cerf and 260 experts give FCC a plan to secure WiFi Routers," Computer World, October 2015.

4. E-Commerce and Development Report, *United Nations Conference on Trade and Development*, 2003, 99.
5. Fred Simon, The future of Open Source: Speeding Technology Innovation, Black Duck Software, 2014.
6. Ghosh RA, "Cooking pot markets: An economic model for the trade in free goods and services on the Internet," *First Monday,* 3 (3), 1998.
7. Jason Williams, Peter Clegg, Emmett Dulaney, "The advantages of adopting Open Source Software," InformIT, May 6,2005 available at http://www.informit.com/articles/article.aspx?p=376255&seqNum=8, (accessed on 09-03-2017).
8. Jurgen Bitzer and Phillip J H Schroder, "The Impact of Entry and Competition by Open Source Software on Innovation Activity," *International Business Section Working Paper Series* no 12 of 2005.
9. Kenneth L. Kraemer, Greg Linden, and Jason Dedrick, "Capturing Value in Global Networks, Apple's iPad and iPhone", *Personal Computing Industry Centre*, 2011.
10. Klint Finley, "Trade Pact Could Bar Governments From Auditing Source Code", *Wired*, Novermber 5 2015.
11. L H Lin, "Impact of user skills and network effects on the competition between open source and proprietary software.," *Electronic Commerce Research and Applications*, Volume 7 Issue No.), 68-81; 2008.
12. M Hobday, "Firm-Level Innovation Models: Perspectives on Research in Developed and Developing Countries," *Technology Analysis & Strategic Management*, Volume 17no.2, pp. 121–146, 2005.
13. Mitchell L. Stoltz, "The Open Source Revolution: Transforming the Software Industry with Help from the Government," *Pomona Senior Theses*, No.7, 2.
14. Nicholas Economides and Evangelos Katsamakas, "Two-Sided Competition of Proprietary vs. Open Source Technology Platforms and the Implications for the Software Industry," *Management Science*, Volume 52 no.7, 2006;
15. P Singh, "A borderless economy that will be controlled" *The Hindu, http://www.thehindu.com/opinion/columns/a-borderless-economy-that-will-be-controlled/article8581476.ece,* 2016 (accessed on 29 January 2017)
16. Ravi Sen, "A Strategic Analysis of Competition Between Open Source and Proprietary Software," *Journal of Management Information Systems* Volume 24 no.1, 2007;
17. Raymond ES, The cathedral and the bazaar. www.catb.org/~esr/writings/cathedral-bazaar, 2000 (accessed on 07.03.2017).
18. Richard Stallman, "The GNU Project," available online at https://www.gnu.org/gnu/thegnuproject.en.html (accessed on 07.03.2017).
19. Richard Stallman, "The GNU Project," available online at https://www.gnu.org/gnu/thegnuproject.en.html (accessed on 07.03.2017).
20. Software Freedom Law Centre, "TPP Article 14.17 & Free Software: No Harm, No Foul," available at https://www.softwarefreedom.org/blog/2015/nov/23/TPP-Article-14/, November 2015.
21. Stephen Shankland, "Is Public Domain Software Open Source?," CNet, available at https://www.cnet.com/news/is-public-domain-software-open-source/
22. Steven Weber, "The Political Economy of Open Source," *BRIE Working Paper* 140, E-conomy Projectä Working Paper, 15 June 2000.
23. Steven Weber, "The Political Economy of Open Source," *BRIE Working Paper* 140, E-conomy Projectä Working Paper, 15 June 2000.
24. Tamir Israel, "TiSA Annex on Electronic Commerce: A Preliminary Analysis," *Canadian Internet Policy and Public Interest Clinic.*

25. W Widenius and N Nyman, "The business of open source software: a primer," *Technology Innovation Management Review*, Volume 1, p8-11, 2014;
26. Zeynep Tufekci, "Volkswagen and the Era of Cheating Software," *The New York Times*, September 23, 2015
27. Declaration on Global Electronic Commerce, *World Trade Organization,* WT/MIN(98)/DEC/2 Ministerial Conference, Geneva, 1998.
28. Non-Paper from EU et al, Work Programme on Electronic Commerce, *World Trade Organization*, JOB/GC/97, July 2016.
29. Non-Paper from Japan, Work Programme on Electronic Commerce, *World Trade Organization*, JOB/GC/100, July 2016.
30. Non-Paper from the United States, Work Programme on Electronic Commerce, *World Trade Organization*, JOB/GC/94, July 2016.