Some preliminary implications of WTO source code proposal – MC11 briefing paper[a]

Introduction

Source code is a computer program written in a high level human readable language[1] such as Fortran or C. ('In contrast, the related object code is the same computer program written in computer readable format, which is required for the program's execution by a computer'[2]). In the current ecommerce discussions at the World Trade Organization (WTO) a number of countries have proposed new rules with similar restrictions on disclosure/transfer/access to source code to those in the Trans-Pacific Partnership (TPP) and Trade In Services Agreement (TISA) apparently without even the TPP or TISA's exceptions.[b] Furthermore, these proposed new ecommerce rules at the WTO do not include any exceptions or special and differential treatment for developing countries or least developed countries (LDCs).

The TPP's ecommerce chapter included a prohibition on TPP governments requiring the transfer of or access to source code.[3] However the TPP also included a number of exceptions to this, including:

[a] By Sanya Reid Smith, Legal Advisor, Third World Network, 10 December 2017.

[b] See for example 4B21 of JOB/GC/97/Rev.3, 4C of JOB/GC/100 and 2.7 of JOB/GC/94 (although the US proposal includes an exception to allow governments to access source code in order to protect health/safety or other legitimate regulatory goals). These WTO documents are available from https://docs.wto.org/dol2fe/Pages/FE_Search/FE_S_S001.aspx. For the purposes of this note, the WTO proposals without any exceptions will be used.

- It only applied to mass-market software/products with mass-market software, so does not apply to software used for critical infrastructure (presumably such as nuclear power plants)[4]
- It does not prevent commercially negotiated contracts (eg between two companies) requiring transfer/access to source code[5]
- It does not affect patent requirements (eg disclosure of source code in order to obtain a patent)
- It does not apply to government procurement (GP)[6] (however this is narrowly defined[c]) or information held/processed by or on behalf of a TPP government or measures related to its collection[7]
- The exceptions in Art XIVa), b), c) of the WTO's General Agreement on Trade in Services (GATS)[8] (for health and environment etc) apply.[9] However this GATS and its equivalent in the General Agreement on Tariffs and Trade (GATT)[10] exceptions have been very difficult to use and governments have only succeeded once out of 44 attempts to use them at the WTO.[11].

The latest leaked TISA text (as of November 2016, after the TPP was signed) has additional/broader exceptions (beyond those in the TPP) to a similar prohibition on requiring the transfer of/access to source code including:

- For free and open source software[12]
- For anticompetitive conduct[13]
- For legitimate public policy objectives, 'provided that such measures are not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or disguised a restriction on trade'[14] (proposed by TISA countries such as Canada which is a cosponsor of the EU et al's WTO source code proposal which does not have these exceptions).

There is currently no mandate to negotiate ecommerce rules at the WTO. At the WTO, the current mandate is merely to examine various ecommerce issues.[15] However, at the WTO Ministerial Conference in Buenos Aires from 10-13 December 2017 (MC11), there is a proposal to begin negotiations on ecommerce rules[16] (presumably such as those above).

There are a number of implications of these source code proposals, some of which have been outlined below. For example a submission to the US government in the context of the equivalent TPP provision pointed out that it has implications for security, privacy, fraud, interoperability and other policies.[17] More research is being done and this note will be updated with that new research.

What is the difference between disclosure of, transfer of and access to source code? These terms are not defined in the TPP or in the proposals at the WTO, but they may mean:

- Disclosure of source code is presumably to the public (or even one other company), eg requiring the source code to be made public for example by putting it online.
- Transfer of source code could be from a foreign investor to a local company
- Access to source code could include by government regulators who need to check that it is not risky for financial regulation, or violating environmental laws etc.

[c] It 'means the process by which a government obtains the use of or acquires goods or services, or any combination thereof, for governmental purposes and not with a view to commercial sale or resale or use in the production or supply of goods or services for commercial sale or resale' Art 1.3 TPP. It is a similarly narrow definition in Art XIII GATS: 'the procurement by governmental agencies of services purchased for governmental purposes and not with a view to commercial resale or with a view to use in the supply of services for commercial sale.' Therefore this kind of narrow government procurement exception may not cover many of the types of procurement by government that need the exception.

How this is TRIMS+

These WTO proposals are effectively a ban on technology transfer requirements, where that technology includes source code (which is increasingly widespread component of technology). Under the Agreement on Trade-Related Investment Measures (TRIMS),[18] WTO Members can still require technology transfer, however these proposals would ban/restrict the ability to require transfer of source code, even though investment is a Singapore issue which cannot be negotiated in the current Doha Round at the WTO[19].

How this is TRIPS+

In addition to being TRIMS+, this proposed source code rule requires stronger intellectual property protection than the rules in the WTO's Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS), ie it is TRIPS+. This is because Art 39 TRIPS[20] only requires WTO Members to allow the trade secret/confidential information owner to sue someone who obtains/uses it etc in a dishonest commercial manner. For example if a Coca Cola employee signed a contract to keep secret his knowledge of Coca Cola's secret recipe, then he resigned from Coca Cola and went to work for Pepsi and told his new employers Coca Cola's secret recipe, this would be a breach of Art 39 TRIPS and Coca Cola could sue him.

The table below indicates the types of laws and policies that can still be required under TRIPS but are prohibited by the WTO's source code proposal (subject to any exceptions).

Some examples of TRIPS flexibilities re source code which are prohibited by the proposed WTO source code provision:

Measure	**Allowed by Art 39 TRIPS?**	**Allowed by WTO proposal?**
Government requires **access** for itself to source code (eg to check car and medical device safety, for financial regulation, for competition or tax laws, to make sure a car is not cheating emissions tests etc)	Y	N
Governments to require **disclosure** of source code eg in a patent application as part of the quid pro quo for getting a patent monopoly (so that others can make the invention after the patent has expired)	Y	N
Governments to require **transfer** of source code for example in technology transfer requirements	Y	N
Courts to require access/disclosure of source code in the discovery process in court cases, or to require transfer of source code as a remedy for anti-competitive conduct	Y	N

Y = yes, N= no

Furthermore, despite least developed countries (LDCs) having the right to repeated transition periods before they have to comply with substantive TRIPS rules such as Art 39.3, essentially until they graduate from being LDCs,[21] no exception for LDCs has been included in these proposed WTO ecommerce rules, so they would be required to provide TRIPS+ intellectual property protection, while they are LDCs.

Why governments may require transfer of source code

There are a number of reasons why governments may want to require transfer of source code. Some examples are below.

Technology transfer

Developing countries and least developed countries (LDCs) may want to require technology transfer (eg from foreign companies to local ones) in order to develop. However, as more products contain software (eg cars, pacemakers, kettles etc), a ban on requiring transfers of source code, would also prevent technology transfer requirements where the technology contains source code.

This goes beyond the WTO's Agreement on Trade-Related Investment Measures (TRIMS) rules.[22]

In 1989, of 31 developing countries studied, 11 had technology transfer requirements.[23]

An example of a technology transfer requirement is in Taiwan where 'In some cases, the government gave approval for investment on the condition that the TNC help its domestic suppliers to upgrade their technology'.[24] Similarly Norway developed expertise in supplying offshore oil rigs[d] via various performance requirements including that 'The licenses also included provisions requiring the transfer of skills and technologies to Norway's infant domestic petroleum industry.'[25]

Local content rules had been a way of obtaining technology transfer in the past.[26] A famous example is the Singer Sewing Machine Company which was allowed into Taiwan in 1964 on condition that Singer must buy 80% of the parts for the sewing machines from Taiwanese companies within one year.[27] To achieve this, the company offered training seminars, provided standard blueprints to its parts producers, supplied them with tools and fixtures, and gave technical assistance and by 1967 Singer's exports used all locally made parts except needles for its straight stitch model.[28] Since requiring local products as inputs is no longer allowed for WTO member countries (except LDCs), countries may instead wish to require technology transfer directly (something which is still allowed by TRIMS), but this would be prohibited by this proposal if it is accepted, for technology containing source code.

As a remedy for anticompetitive conduct

If a company has been found to be anticompetitive (eg by the courts, an administrative tribunal or the competition authority) under a country's competition law (including due to a merger/acquisition), it may order the transfer of source code (or products/services/technology containing the source code) to competitors as a remedy. For example the US government's competition authority (the Federal Trade Commission) ordered MSC to transfer source code (by a royalty-free compulsory licence) as a penalty for violating antitrust laws by eliminating competition and monopolizing the market for advanced versions of its software when it acquired its only competitors.[29]

[d] 'When oil was first discovered offshore in 1969, Norway did not have the expertise to supply offshore oil rigs. But within roughly thirty years, companies were sourcing more than 50% of capital inputs and more than 80% of operations and maintenance inputs from Norwegian firms. The acquired expertise has also enabled Norwegian firms to expand into export markets, with exports comprising nearly half of their sales by the early 2000s. Norway achieved these results through a mix of various measures' including technology transfer requirements and 'It is estimated that in 2014 the oilfield services industry was one of the largest contributors to the Norwegian economy with 1,100 companies employing 122,000 people.' GIZ, Lise Johnson, July 2016, *Space for Local Content Policies and Strategies – A crucial time to revisit an old debate,* https://www.giz.de/expertise/downloads/giz2016-en-local-content-policies-study.pdf

Tax law

In some countries such as the USA, tax authorities have the power to copy the source code of software used for accounting, tax return preparation or compliance, or tax planning (and remove it from the owner's place of business if ordered by a court), if necessary for analysis.[30] It is unclear if there would be a sufficient tax exception to these proposed rules on source code at the WTO or in free trade agreements (FTAs).

In government procurement

When governments are buying any product/service containing software, both developed and developing country governments often want the source code so that they can have competitive tendering for upgrades and modifications to the software without being locked into only buying from the original supplier (who could charge a monopoly price) since only the original supplier has the source code.

It is unclear if these types of contractual specifications in this situation would be covered by the TPP ecommerce chapter's exception for GP given the narrow definition of GP as the 'process'[31].

Why governments may require access to source code

Access to source code is needed for effective regulation in various areas. For example, in the context of the Volkswagen emissions scandal where Volkswagen used software to defeat the emissions test and pollute up to 40 times the legal limit when being driven in the real world, a US computer science associate professor[32] writing in the New York Times noted that:

> 'In a world where more and more objects are run by software, we need to have better ways to catch such cheaters. . .
>
> Corporate cheating is not novel: that's why we have regulations to oversee the quality of many objects, ranging from lead in paint to pesticide residue in food. If similar 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. . .
>
> This isn't the first instance of a car company caught cheating by using a "defeat device" on emissions tests. In 1998, Ford was fined $7.8 million for using defeat devices that allowed its Econoline vans to reduce emissions to pass testing, and then to exceed pollution limits when driving at highway speeds. The same year, Honda paid $17.1 million in fines for deliberately disabling a "misfire" device that warned about excess emissions. In 1995, General Motors paid $11 million in fines for the "defeat devices" on some of its Cadillac cars, which secretly overrode the emissions control system at times. The largest penalty for defeat devices to date was an $83.4 million fine in 1998 on Caterpillar, Volvo, Renault and other manufacturers.'[33]

To solve this, she said that research must be allowed into this software for example by 'creating special commissions with full access to the code under regulatory supervision' and she noted that:

> 'None of this is impossible. There is one industry in particular that employs many of these safeguards in an admirable fashion: slot machines in casinos. These machines, which in some ways present the perfect cheating scenario, are run by software designed by the manufacturers without a centralized database of winnings and losses to check if frequencies of losses are excessive. Despite all these temptations, in many jurisdictions, these machines run some of the best regulated software in the country. The machines are legally allowed to win slightly more often than lose, of course, ensuring a tidy profit for the casinos (and tax revenues for the local governments) without cheating on the disclosed standards.
>
> It's a pity that casinos have better scrutiny of their software than the code running our voting machines, cars and many other vital objects, including medical devices and even our infrastructure. As computation spreads in society, our regulatory systems need to be funded

appropriately and updated in their methods so that keeping our air clean and our elections honest is not a worse gamble than a slot machine.'[34]

In addition to the areas listed below, a New Zealand law professor has noted other areas of law which can be undermined by the TPP's source code provision.[35]

Competition law

'The United States has on more than one occasion required software publishers to open parts of their software code, in order to address competition concerns.'[36] Access to source code can be part of various aspects of competition law including:

- In competition investigations. For example,
    - Law Professor Pasquale provided examples of Google's competitors (such as a price comparison website) whose results were downranked in Google searches and who had to pay 5 pounds in an ad bid instead of 5 pence. In explaining the difficulties of determining whether this was anticompetitive behaviour, Law Professor Pasquale concluded that 'Agencies ought to be able to "look under the hood" of highly advanced technologies like the algorithms at the heart of the Google search engine and the data they process.'[37]
    - as the EU found, Google designs its algorithm to promote its own products in an abuse of dominance.[38] While this can be determined in some cases by doing tests with dummies etc, some platforms such as Facebook require real names[39] and so do not allow dummy tests and so the only way to find abuse of dominance etc in their algorithms is to inspect their source code.
    - Some competition laws allow the competition authority to access/seize/inspect anything including source code.[40]
- As a condition of a proposed merger. For example, 'Access to the source code of MySQL was a major issue in the EU competition review of the Oracle acquisition of Sun Microsystems'.[41]

Tax law

In some countries such as the USA, tax authorities have the power to access and analyse the source code of software used for accounting, tax return preparation or compliance, or tax planning in certain circumstances such as if it cannot otherwise reasonably ascertain the correctness of any item on a return.[42] The US tax authority also has the power to take the source code away and disclose it to certain persons.[43] It is unclear if there would be a sufficient tax exception to these proposed rules on source code at the WTO or in free trade agreements (FTAs).

Financial regulation

The US Securities and Exchange Commission and Commodity Futures Trading Commission have access to high frequency trading (HFT) source code[44] since HFT can destabilise the stock market by exacerbating flash crashes[e] etc[45].

Even if the GATS prudential defence applies to the proposed restrictions on accessing source code, because it has a self-cancelling 2nd sentence ('Where such measures do not conform with the provisions of the Agreement, they shall not be used as a means of avoiding the Member's commitments or obligations under the Agreement'),[46] governments such as the European Union (EU) and USA have not relied on it in some of their FTAs. Eg:

- in the TPP, US financial regulators did not appear to think that this prudential defence would be enough to allow them to require financial data to be stored locally so they could access it in time

[e] Flash crashes are caused due to a rapid fall in price in a very short period of time, mostly occurring due to high speed automated trading. A number of governments are therefore looking at regulating HFT, eg India: http://uk.businessinsider.com/sebi-considering-measures-to-slow-down-hft-2016-7?r=US&IR=T, http://www.sebi.gov.in/sebi_data/attachdocs/1470393485587.pdf

in a financial crisis[47] (eg to unwind positions held by Lehman Brothers when it collapsed and the data was held in Hong Kong but the IT systems had been switched off and the IT staff left[48]), even though it applies to the ecommerce chapter, so they insisted on explicitly excluding financial data from the prohibition on requiring data to be stored locally in the TPP's ecommerce chapter[f].

- In some EUFTAs eg the Canada-EU FTA (CETA)[49] and Article 104 of the EU-CARIFORUM EPA[50] the second self-cancelling sentence of the GATS prudential defence has been deleted because presumably those governments thought it made the exception ineffective.

Car safety

Source code may need to be checked by regulators and outside experts to identify problems causing fatal accidents. For example, when the brakes in Toyota cars suddenly stopped working causing fatal crashes, a US government agency[51] enlisted experts to check the software and the plaintiff's experts in a court case against Toyota also examined the source code and found the problem that caused the fatal crashes.[52]

Court cases

Access to source code has been requested and ordered in a wide variety of court cases. For example:

- a court has ordered Waymo's counsel and expert to have access to Uber's source code to see if it was stolen from Google[53]
- intellectual property infringement cases,[54] for example court ordered production of the source code.[55]
- a court unsealed the source code used to for DNA matching in criminal cases[56]
- a court ordered the disclosure of the source code in a breathalyser so the alleged drunk driver could check its accuracy.[57]

Gambling regulation

As noted above, a number of governments regulate the software in slot machines in casinos to make sure that gamblers can win sometimes. For example, the Nevada gambling regulator requires access to source code of gaming machines.[58]

Anti-discrimination law

The senior technologist at the US government's Federal Trade Commission found that African Americans were being unfairly targeted by an online service.[59] When she searched for her own name (Latanya Sweeney), she saw ads saying 'Latanya Sweeney arrested?', but a search for 'Tanya Smith' showed ads for 'located: Tanya Smith'.[60] When she conducted a study, she found that Google searches for typically African American names lead to statistically significant discrimination in ad delivery because they led negative ads posted by the background check site Instant Checkmate.com (even when there was no actual arrest record), while typically Caucasian names draw neutral ads.[61] So if an employer is doing an online check of job applicants, African American names would show ads for arrest records etc rather than neutral ads. Google and Instant Checkmate denied anyone had deliberately programmed 'arrest' results to appear with names associated with African Americans (which would be intentional discrimination), for example it could have arisen from other associations in the data.[62] Law Professor Pasquale concluded that 'without access to the underlying coding and data, it is nearly impossible to adjudicate the dispute.'[63]

Similarly, a researcher created a small number of test Gmail accounts and compared the ad results when he sent emails about car shopping to and from the test accounts. He found that 'all three white names yielded car buying sites of various kinds. . . Conversely, all three of the African-American

[f] Art 14.1 TPP: definition of 'covered person' 'does not include a "financial institution" or a "cross-border financial service supplier of a Party"

names yielded at least one ad related to bad credit card loans'.[64] Pasquale again concluded that without access to the underlying data and code, it is not possible to know what kind of tracking of African Americans into one set of online opportunities and whites into another is occurring.[65]

The algorithm in the sentencing software in the USA was biased against African Americans[66] and this type of discrimination may not be detectable without checking the source code.

US law prohibits discriminatory advertisements in housing, employment and credit.[67] However:

- an investigation found that Facebook repeatedly allowed ads for houses for rent that would not be shown to African Americans, Jews and Spanish speakers etc, which violates the US Fair Housing Act.[68]
- An Ad Fisher study by Carnegie Mellon University found that 'when Google presumed users to be male job seekers, they were much more likely to be shown ads for high-paying executive jobs. Google showed the ads 1,852 times to the male group — but just 318 times to the female group . . [when] the accounts used were more or less identical, except for their listed gender identity. That would seem to indicate either that advertisers are requesting that high-paying job ads only display to men (and that Google is honoring that request) or that some type of bias has been programmed, if inadvertently, into Google's ad-personalization system.'[69]
- As noted above, without checking the source code, it may not be possible to discover whether this is deliberate discrimination.

Minimising vulnerabilities to hacking

This is not a comprehensive survey, but just some examples from recent news reports of the types of things that can be/have been hacked and so the government may want/need access to the source code to check it is not vulnerable to hacking in the future. Many other public (and not publicly known) examples have occurred and should be comprehensively reviewed to ensure that regulations are allowed to at least deal with all the past types of attacks.

However this is a fast moving field and as the experts note below:

- More things will be connected to the internet (eg by 2020 one estimate is 50 billion devices and objects will be connected to the internet[70]) and so be hackable (internet of things)
- more hacks are likely[71] and
- the hacks will be more damaging.

Therefore if these types of source code rules are agreed to, a limited list of exceptions is unlikely to be sufficient to even cover the new hacks that occur between the conclusion of any rules on source code and their entry into force, let alone for the life of the rules.

Products that can harm health

- Pacemakers and insulin pumps[72] are hackable and the US government's Food and Drug Administration issued guidelines on this in December 2016 which gave an example of 'A manufacturer becomes aware of a vulnerability via a researcher that its class III medical device (e.g., implantable defibrillator, pacemaker, etc.) can be reprogrammed by an unauthorized user. If exploited, this vulnerability could result in permanent impairment, a life-threatening injury, or death.'[73] The Australian government's medical device regulator is also concerned about the vulnerability of medical devices to hacking.[74]
- Cars are hackable (brakes can be turned off, engine stopped, steering affected etc) according to the US government's Federal Bureau of Investigation (FBI) in March 2016.[75]

Critical infrastructure hacked

- Nuclear power plants have been hacked.[76]

- San Francisco's public transport ticketing system was hacked resulting in free rides for passengers.[77] Would this count as 'critical infrastructure' under any critical infrastructure exception?

Internet of things used to launch a broader attack

For example:

- 2014: 'a fridge, home routers and smart TVs were among 100,000 devices hacked to launch a spam email campaign.'[78]
- In October 2016 hundreds of thousands of internet connected devices were hacked and used to take down sites such as Paypal, Twitter and Spotify.[79] Internet of things devices such as baby monitors etc are not manufactured with enough memory to be able to be made secure.[80]

Since many more hacks are likely, experts recommend governments to regulate the internet of things more securely, eg Gabriella Coleman, the Wolfe chair in scientific and technological literacy at McGill University: "Given the magnitude of this attack, let's hope it can serve as a wake-up call, forcing government officials to more aggressively regulate the production of these devices so that companies are forced to make security a priority."[81]

Summary of examples and whether the TPP's exceptions would be sufficient for the known scenarios above

The EU et al and Japanese source code proposals at the WTO have no proposed exceptions to their rules. Even if the TPP's limited exceptions to source code were included in the proposed WTO rules, it would not be enough to even cover the hacked situations that are known about today, let alone future problems and those in other areas (eg see rest of this paper).

Type of known hack	**TPP's exceptions would cover this situation? If so, which exception?**
Pacemakers and other medical devices: FDA guidelines December 2016	Since these are mass market products, the critical infrastructure exception would not apply. This does not involve government procurement either, so the health exception in the TPP's general exceptions would need to be used (although it has not been very successful at the WTO, see above)
Cars hackable – FBI warning March 2016	Since these are mass market products, the critical infrastructure exception would not apply. This does not generally involve government procurement either, so the health exception in the TPP's general exceptions would need to be used (although it has not been very successful at the WTO, see above)
Korean nuclear power plant hacked in 2014	This would presumably be covered by the critical infrastructure exception
Public transport ticketing system hacked in December 2016	This may not be 'critical infrastructure' and so not covered by the critical infrastructure exception. This is unlikely to be covered by the definition of 'government procurement' in the TPP since the public pays for it (even if it covered subnational procurement which is not clear) and it is not health/environment etc under the general exceptions. So there appears to be no exception in the TPP to allow governments to require access to source code in this type of product to check it is not vulnerable to hacking.
Mass attacks by internet of things in 2014 (and 2016)	Since the devices that were hacked are mass market products such as fridges and TVs this would not be covered by the critical infrastructure

	exception (even if thousands of hacked fridges were then used to launch an attack on critical infrastructure such as a nuclear power plant). This situation would also not be covered by the health/environment/GP etc exceptions, so there appears to be no exception in the TPP to allow governments to require access to source code in this type of product to check it is not vulnerable to hacking.
Volkswagen was found to have used software to circumvent US emissions standards in September 2015[82]	This is not critical infrastructure (nor is it generally GP), so it would need to use the TPP's exceptions chapter general environment exception. However this environment exception has been very difficult to use, see above.
Examples of discrimination in software (from 2014-2016)	This would not be covered by the TPP exceptions because even the court sentencing software is not GP since GP is defined in the TPP[g] to only be the process of buying the software, not the final software purchased.

Those in grey occurred after the TPP text was concluded on 6 October 2015.

Sensitive products including in government procurement

A number of governments have been concerned that several U.S.-based technology companies like Cisco and Apple may have installed so-called back doors into their products based on leaks by whistleblower Edward Snowden that exposed U.S. espionage activities.[83] Therefore some governments 'are asking Western tech companies to allow them to review source code for security products such as firewalls, anti-virus applications and software containing encryption before permitting the products to be imported and sold in the country.'[84]

Why governments may require disclosure of source code

There are a variety of reasons why governments may require disclosure of source code, including to the public. For example:

- In some countries such as the USA, tax authorities have the power to disclose the source code of software used for accounting, tax return preparation or compliance, or tax planning to certain people for tax administration purposes.[85] It is unclear if there would be a sufficient tax exception to these proposed rules on source code at the WTO or in free trade agreements (FTAs).
- Part of the bargain underlying the exception to the competition norm for patent monopolies is that the invention being patented is made public so that after the patent expires, others can make it and improve on it etc.[86] If the invention involves source code, the prohibition on disclosing it means that patent laws will have to be changed so that a patent involving source code will be granted without the inventor having to disclose the invention, which means that society provides a patent monopoly without getting disclosure of the invention in return.
- Courts have ordered disclosure of source code (for example due to public interest in the accuracy of DNA matching in criminal cases and so that others who were convicted due to evidence using this software could also check its accuracy[87]).
- Some countries require open source software for their voting machines because it is more secure and transparent.[88] For example:
    - An Australian territory uses open source software on its voting machines. sAs the electoral commission for the Australian Capital Territory explained: 'going the open-source route was an obvious choice. "We'd been watching what had happened in America (in 2000), and we were wary of using proprietary software that no one was allowed to see," he said. "We were very keen for the whole process to be transparent so that

[g] Definition of GP in Art 1.3 TPP which is used in the GP exception in 14.2.3a)

everyone – particularly the political parties and the candidates, but also the world at large – could be satisfied that the software was actually doing what it was meant to be doing."'[89]

- Geneva's internet voting system includes open source software and 'The Geneva law opens the code for review by the electoral commission or by any expert it designates. It also foresees access to the code by anyone having a scientific interest'.[90]
- In Brazil, 'Six months prior to any election, people who have been accredited by the Court are allowed to come in-person, "in an environment controlled by the Superior Electoral Court," where experts can examine the source code, under a nondisclosure agreement.'[91] One of the experts (a computer science professor) who examined the Brazilian voting machine source code under this system and found a flaw wrote in an academic paper that 'The necessity of installing a scientifically sound and continuous evaluation of the system, performed by independent specialists from industry or academia becomes evident and should contribute to the improvement of the security measures adopted by the voting equipment.'[92] Depending on how this examination works, this could be characterised as a **transfer** of the source code from the developers to the Brazilian government so they can **disclose** the source code to these experts who have **access** to it. Therefore the differences between these verbs may not be clear. If any GP exception is the narrow TPP type, it may not cover this.
- A bill has been proposed in the USA to make the source code for voting machines open to the public.[93]

However this requirement to use open source software may not be possible if there is a ban on disclosure of source code,[94] (especially if any exception for GP is the narrow TPP-type, see above).

- If a standard has been set (eg USB ports for computers) that all manufacturers have to meet and that involves software, then the government may want to require disclosure of that software so that manufacturers can meet the standard and make interoperable parts.
- Arguably government requirements to use open source software (eg the US Department of Defense because it is more secure (see Annex)), may violate a prohibition on disclosure of software as condition of selling the product (to the government). (As noted above, TISA has an exception for open source software which shows that TISA governments were concerned that the ecommerce source code provision could harm open source software). Furthermore, it is unclear whether this would be covered by the GP exception since such specifications or the software purchased may not be part of the GP 'process', see above.

Annex: open source software

Governments may want to use open source software for a number of reasons including that it is cheaper and according to some experts, open source software (OSS) is more secure.[95] Keeping the source code secret does not make it more secure according to the US government's Department of Defense[96]: 'vulnerability databases such as CVE make it clear that merely hiding source code does not counter attacks:

- Dynamic attacks (e.g., generating input patterns to probe for vulnerabilities and then sending that data to the program to execute) don't need source or binary. Observing the output from inputs is often sufficient for attack.
- Static attacks (e.g., analyzing the code instead of its execution) can use pattern-matches against binaries - source code is not needed for them either.
- Even if source code is necessary (e.g., for source code analyzers), adequate source code can often be regenerated by disassemblers and decompilers sufficiently to search for vulnerabilities. Such source code may not be adequate to cost-effectively *maintain* the software, but attackers need not maintain software.

- Even when the original source is necessary for in-depth analysis, making source code available to the public significantly aids defenders and not just attackers. Continuous and broad peer-review, enabled by publicly available source code, improves software reliability and security through the identification and elimination of defects that might otherwise go unrecognized by the core development team. Conversely, where source code is hidden from the public, attackers can attack the software anyway as described above. In addition, an attacker can often acquire the original source code from suppliers anyway (either because the supplier voluntarily provides it, or via attacks against the supplier); in such cases, if only the attacker has the source code, the attacker ends up with another advantage.

Hiding source code *does* inhibit the ability of third parties to respond to vulnerabilities (because changing software is more difficult without the source code), but this is obviously *not* a security advantage. In general, "Security by Obscurity" is widely denigrated.'

http://dodcio.defense.gov/Open-Source-Software-FAQ/ answers common questions about OSS eg:

- that OSS is developed by experts,
- that the US Government's Department of Defense already uses OSS eg see http://dodcio.defense.gov/Portals/0/Documents/OSSFAQ/dodfoss_pdf.pdf,
- that both proprietary and OSS can have malicious code in it: 'The use of *any* commercially-available software, be it proprietary or OSS, creates the risk of executing malicious code embedded in the software. Even if a commercial program did not originally have vulnerabilities, both proprietary and OSS program binaries can be modified (e.g., with a "hex editor" or virus) so that it includes malicious code. It may be illegal to modify proprietary software, but that will normally not slow an attacker. Thankfully, there are ways to reduce the risk of executing malicious code when using commercial software (both proprietary and OSS).. . many people have released proprietary code that is malicious. What's more, proprietary software release practices make it more difficult to be confident that the software does not include malicious code. Such software does not normally undergo widespread public review, indeed, the source code is typically not provided to the public and there are often license clauses that attempt to inhibit review further . . . [In OSS] such malicious code cannot be directly inserted by "just anyone" into a well-established OSS project. As noted above, OSS projects have a "trusted repository" that only certain developers (the "trusted developers") can directly modify. In addition, since the source code is publicly released, anyone can review it, including for the possibility of malicious code. The public release also makes it easy to have copies of versions in many places, and to compare those versions, making it easy for many people to review changes. Many perceive this openness as an advantage for OSS, since OSS better meets Saltzer & Schroeder's "Open design principle" ("the protection mechanism must not depend on attacker ignorance"). This is not merely theoretical; in 2003 the Linux kernel development process resisted an attack. Similarly, SourceForge/Apache (in 2001) and Debian (in 2003) countered external attacks.. . . The example of Borland's InterBase/Firebird is instructive. For at least 7 years, Borland's Interbase (a proprietary database program) had embedded in it a "back door"; the username "politically", password "correct", would immediately give the requestor complete control over the database, a fact unknown to its users. Whether or not this was intentional, it certainly had the same form as a malicious back door. When the program was released as OSS, within 5 months this vulnerability was found and fixed. This shows that proprietary software can include functionality that could be described as malicious, yet remain unfixed - and that at least in some cases OSS is reviewed and fixed.' http://dodcio.defense.gov/Open-Source-Software-FAQ/#Q:_Is_there_a_risk_of_malicious_code_becoming_embedded_into_OSS.3F

Free/Open Source Software (OSS) has been preferred by the US military from 2002 onwards and this position has not changed to date. Eg see 2009 US government memo re why they prefer OSS: http://dodcio.defense.gov/Portals/0/Documents/FOSS/2009OSS.pdf. See also http://dodcio.defense.gov/Portals/0/Documents/FOSS/OTD-lessons-learned-military-signed.pdf.

[1] http://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?article=1300&context=chtlj
[2] http://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?article=1300&context=chtlj
[3] Art 14.17.1 http://tpp.mfat.govt.nz/text
[4] Art 14.17.2
[5] Art 14.17.3a
[6] Art 14.2.3a
[7] Art 14.2.3b
[8] https://www.wto.org/english/docs_e/legal_e/26-gats_01_e.htm#articleXIV
[9] Art 29.1.3
[10] https://www.wto.org/english/docs_e/legal_e/gatt47_02_e.htm#articleXX
[11] https://www.citizen.org/documents/general-exception.pdf
[12] Article 6, http://bilaterals.org/IMG/pdf/ecommercenonpapersmallgroup.pdf.
[13] Article 6, http://bilaterals.org/IMG/pdf/ecommercenonpapersmallgroup.pdf.
[14] Article 6.2, http://bilaterals.org/IMG/pdf/annex_on_electronic_commerce.pdf
[15] WT/L/274 from https://docs.wto.org/dol2fe/Pages/FE_Search/FE_S_S001.aspx.
[16] WT/MIN(17)/15 from https://www.wto.org/english/thewto_e/minist_e/mc11_e/documents_e.htm
[17] https://www.keionline.org/wp-content/uploads/KEI-USITC-TPP-29Dec2015.pdf
[18] https://www.wto.org/english/docs_e/legal_e/18-trims_e.htm
[19] WT/L/579 from https://docs.wto.org/dol2fe/Pages/FE_Search/FE_S_S001.aspx
[20] https://www.wto.org/english/docs_e/legal_e/31bis_trips_01_e.htm
[21] Art 66.1 TRIPs, https://www.wto.org/english/docs_e/legal_e/31bis_trips_01_e.htm
[22] https://www.wto.org/english/docs_e/legal_e/18-trims_e.htm
[23] UNCTAD 2003, *Foreign direct investment and performance requirements : New evidence from selected countries*, UNCTAD/ITE/IIA/2003/7,http://unctad.org/en/Docs/iteiia20037_en.pdf
[24] The European Journal of Development Research, Vol.16, No.3, Autumn 2004, pp.687–715, Ha-Joon Chang, *Regulation of Foreign Investment in Historical Perspective,* http://law.wisc.edu/gls/documents/foreign_investment1.pdf
[25] GIZ, Lise Johnson, July 2016, *Space for Local Content Policies and Strategies – A crucial time to revisit an old debate,* https://www.giz.de/expertise/downloads/giz2016-en-local-content-policies-study.pdf
[26] Eg Stephan Haggard and Yu Zheng, *Institutional Innovation and Private Investment in Taiwan,* 'Singer was subject to stringent local content requirements that could only be met through effective technology transfer to suppliers', http://siteresources.worldbank.org/INTEXPCOMNET/Resources/Institutional_Innovation_and_Private_Investment_in_Taiwan.doc
[27] Oxfam International,Watkins Kevin and Fowler Penny, 01 May 2002, *Rigged Rules and Double Standards: Trade, globalization and the fight against poverty,* http://policy-practice.oxfam.org.uk/publications/rigged-rules-and-double-standards-trade-globalisation-and-the-fight-against-pov-112391
[28] Myers, Ramon H. "The Economic Transformation of the Republic of China on Taiwan." The China Quarterly, No. 99 (Sept. 1984): 517.
[29] https://www.ftc.gov/news-events/press-releases/2002/08/mscsoftware-settles-ftc-charges-divesting-nastran-software
[30] 26 U.S. Code § 7612 - Special procedures for summonses for computer software, https://www.law.cornell.edu/uscode/text/26/7612
[31] Art 1.3 TPP
[32] https://sils.unc.edu/people/faculty/zeynep-tufekci
[33] https://www.nytimes.com/2015/09/24/opinion/volkswagen-and-the-era-of-cheating-software.html?_r=0
[34] https://www.nytimes.com/2015/09/24/opinion/volkswagen-and-the-era-of-cheating-software.html?_r=0
[35] at page 37 (hard copy page numbering) of http://www.eria.org/publications/discussion_papers/DP2017-10.html
[36] https://www.keionline.org/wp-content/uploads/KEI-USITC-TPP-29Dec2015.pdf
[37] 'The Black Box Society: the secret algorithms that control money and information', Frank Pasquale, Harvard University Press, 2015
[38] http://europa.eu/rapid/press-release_IP-17-1784_en.htm
[39] https://www.facebook.com/terms.php
[40] For example Canada: http://www.laws.justice.gc.ca/eng/acts/C-34/index.html and Malaysia: http://www.mycc.gov.my/sites/default/files/CA2010.pdf
[41] http://ec.europa.eu/competition/mergers/cases/decisions/m5529_20100121_20682_en.pdf from https://www.keionline.org/wp-content/uploads/KEI-USITC-TPP-29Dec2015.pdf

[42] 26 U.S. Code § 7612 - Special procedures for summonses for computer software, https://www.law.cornell.edu/uscode/text/26/7612
[43] 26 U.S. Code § 7612 - Special procedures for summonses for computer software, https://www.law.cornell.edu/uscode/text/26/7612
[44] https://www.bna.com/doddfrank-redo-limit-n57982086612/
[45] https://www.wsj.com/articles/german-bundesbank-high-frequency-trading-can-worsen-flash-crashes-1477306280
[46] https://www.wto.org/english/docs_e/legal_e/26-gats_02_e.htm#annfin
[47] http://www.politico.com/tipsheets/morning-trade/2016/02/lew-defends-financial-services-data-carveout-senate-to-vote-on-customs-bill-democrats-weigh-in-on-tpp-212657
[48] http://www2.itif.org/2016-financial-data-trade-deals.pdf?mc_cid=0a36b6ab0c&mc_eid=671b585ee6
[49] http://trade.ec.europa.eu/doclib/docs/2016/february/tradoc_154329.pdf (Art 13.16.1 on p103)
[50] (signed in 2008: http://ec.europa.eu/trade/policy/countries-and-regions/regions/caribbean/) http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:289:0003:1955:EN:PDF
[51] https://www.nhtsa.gov/about-nhtsa
[52] https://www.theatlantic.com/technology/archive/2017/09/saving-the-world-from-code/540393/
[53] https://arstechnica.com/wp-content/uploads/2017/05/Uber.Waymo_.Order_.pdf
[54] For example https://www.forbes.com/sites/johnvillasenor/2014/05/19/how-much-copyright-protection-should-source-code-get-a-new-court-ruling-reshapes-the-landscape/#4c09789e3cf7
[55] http://www.haynesboone.com/publications/source-code-found-too-late-in-software-copyright-infringement-case
[56] https://www.propublica.org/article/propublica-seeks-source-code-for-new-york-city-disputed-dna-software and then https://www.propublica.org/article/federal-judge-unseals-new-york-crime-labs-software-for-analyzing-dna-evidence
[57] Eg https://www.wired.com/2009/05/minnesota-court-release-source-code-of-breath-testing-machines/ and https://digital.law.washington.edu/dspace-law/bitstream/handle/1773.1/1069/7WJLTA123.pdf?sequence=4
[58] 14.030.5c) and 14.110.3c)1) http://gaming.nv.gov/modules/showdocument.aspx?documentid=2921
[59] 'The Black Box Society: the secret algorithms that control money and information', Frank Pasquale, Harvard University Press, 2015
[60] 'The Black Box Society: the secret algorithms that control money and information', Frank Pasquale, Harvard University Press, 2015
[61] Latanya Sweeney, 'Discrimination in Online Ad Delivery', Communications of the ACM 56 (2013): 44
[62] 'The Black Box Society: the secret algorithms that control money and information', Frank Pasquale, Harvard University Press, 2015
[63] 'The Black Box Society: the secret algorithms that control money and information', Frank Pasquale, Harvard University Press, 2015
[64] https://www.huffingtonpost.com/nathan-newman/racial-and-economic-profi_b_970451.html
[65] 'The Black Box Society: the secret algorithms that control money and information', Frank Pasquale, Harvard University Press, 2015
[66] https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing?utm_source=suggestedarticle&utm_medium=referral&utm_campaign=readnext&utm_content=https%3A%2F%2Fwww.propublica.org%2Farticle%2Fmachine-bias-risk-assessments-in-criminal-sentencing
[67] https://www.propublica.org/article/facebook-advertising-discrimination-housing-race-sex-national-origin
[68] https://www.propublica.org/article/facebook-advertising-discrimination-housing-race-sex-national-origin
[69] http://www.independent.co.uk/life-style/gadgets-and-tech/news/googles-algorithm-shows-prestigious-job-ads-to-men-but-not-to-women-10372166.html
[70] http://www.worldbank.org/en/publication/wdr2016
[71] http://www.cbc.ca/news/technology/internet-ddos-attack-analysis-1.3820297
[72] http://www.nbcnews.com/health/health-news/insulin-pump-vulnerable-hacking-johnson-johnson-warns-n659221
[73] https://www.fda.gov/ucm/groups/fdagov-public/@fdagov-meddev-gen/documents/document/ucm482022.pdf
[74] Eg see https://www.tga.gov.au/publication-issue/medical-devices-safety-update-volume-4-number-2-march-2016
[75] https://www.ic3.gov/media/2016/160317.aspx
[76] For example https://www.theguardian.com/world/2014/dec/22/south-korea-nuclear-power-cyber-attack-hack
[77] http://www.nbcnews.com/tech/security/who-s-next-after-san-francisco-s-public-transit-system-n689216
[78] https://www.theguardian.com/technology/2016/oct/22/smart-devices-too-dumb-to-fend-off-cyber-attacks-say-experts

[79] https://www.theguardian.com/technology/2016/oct/22/smart-devices-too-dumb-to-fend-off-cyber-attacks-say-experts
[80] https://www.theguardian.com/technology/2016/oct/22/smart-devices-too-dumb-to-fend-off-cyber-attacks-say-experts
[81] http://www.cbc.ca/news/technology/internet-ddos-attack-analysis-1.3820297
[82] https://www.epa.gov/newsreleases/epa-california-notify-volkswagen-clean-air-act-violations-carmaker-allegedly-used
[83] http://fortune.com/2016/09/19/microsoft-china-transparency-center-beijing/
[84] https://www.reuters.com/article/us-usa-russia-tech-insight/under-pressure-western-tech-firms-bow-to-russian-demands-to-share-cyber-secrets-idUSKBN19E0XB
[85] 26 U.S. Code § 7612 - Special procedures for summonses for computer software, https://www.law.cornell.edu/uscode/text/26/7612
[86] See for example https://www.uspto.gov/sites/default/files/documents/uspto_112a_part1_17aug2015.pptx.
[87] https://www.propublica.org/article/propublica-seeks-source-code-for-new-york-city-disputed-dna-software, https://www.propublica.org/article/federal-judge-unseals-new-york-crime-labs-software-for-analyzing-dna-evidence
[88] https://www.wired.com/2003/11/aussies-do-it-right-e-voting/
[89] https://www.wired.com/2003/11/aussies-do-it-right-e-voting/
[90] https://www.coe.int/t/dgap/goodgovernance/activities/e-voting/evoting_documentation/passport_evoting2010.pdf
[91] https://arstechnica.com/features/2016/11/internet-based-and-open-source-how-e-voting-is-working-around-the-globe/
[92] https://arstechnica.com/features/2016/11/internet-based-and-open-source-how-e-voting-is-working-around-the-globe/
[93] https://www.wired.com/2003/11/aussies-do-it-right-e-voting/
[94] http://wtocentre.iift.ac.in/workingpaper/Working%20Paper%2037.pdf
[95] https://www.schneier.com/crypto-gram/archives/1999/0915.html#OpenSourceandSecurity
[96] http://dodcio.defense.gov/Open-Source-Software-FAQ/#Q:_Doesn.27t_hiding_source_code_automatically_make_software_more_secure.3F