

Why Do We Need Encryption Rules in the TPP?

Takaaki Sashida¹ | September 2013

A key priority for the U.S. semiconductor industry regarding the Trans-Pacific Partnership (TPP) Agreement currently under negotiation has been to introduce rules to prevent restrictions on the import and use of commercial encryption technologies. Why is this seemingly obscure issue considered so important by a major industry?

There are three main reasons:

- 1) Commercial encryption is both increasingly ubiquitous in every day Information and Communication Technology (ICT) products and inseparable from the presence of semiconductors.
- 2) Large trade flows of semiconductors and other ICT products, easily reaching the scale of tens of billions of dollars, could be threatened by the adoption of restrictive policies in a few key emerging economies.
- 3) Existing trade rules contain too many gray areas to provide effective insurance against such policy changes.

While the inclusion of effective rules in the TPP will need to be followed up with further initiatives to head off the threat of trade restrictive encryption policies, it is nonetheless a key first step. Thus, if the effort is successful, it will be a good example of the value-added that the TPP can provide as a “21st century trade agreement.”

THE TPP: OVERVIEW OF IMPLICATIONS FOR THE SEMICONDUCTOR INDUSTRY

The TPP is a comprehensive Free Trade Agreement under negotiation by the United States and Asia-Pacific nations. On July 23rd, 2013, Japan became the 12th participant in the talks.² The SIA has welcomed Japan's inclusion "[g]iven Japan's status as a top semiconductor trading partner, and a valued member of the world trading community."³

“The inclusion of newer issues such as non-tariff barriers to trade that apply to digital products, strong protection of intellectual property rights, foreign participation in domestic standard setting activities, and anti-counterfeiting measures are vital for the TPP Agreement to deliver commercially meaningful results once finalized.”

Japan's entry provides an opportunity to reflect on the potential benefits of the TPP for the semiconductor industry, in particular its “21st century” provisions. With regard to semiconductors, many of the traditional issues in trade talks have already been addressed to a large extent. In particular, almost all tariffs have been eliminated through initiatives such as the Information Technology Agreement (ITA), although some important issues remain.⁴ Thus, in the industry's view, the inclusion of newer issues such as non-tariff barriers to trade that apply to digital products, strong protection of intellectual property rights, foreign participation in domestic standard setting activities, and anti-counterfeiting measures are vital for the TPP Agreement to deliver commercially meaningful results once finalized.⁵

Reining in restrictive encryption policies is one such new issue. Below, I will briefly explain the nature of such policies and how one can conceptualize different encryption policies based on the way they affect trade, before analyzing the potential adverse impact of various new policies, as well as why existing trade rules are likely to be insufficient.

WHAT IS ENCRYPTION AND HOW IS IT USED TODAY?

Roughly speaking, encryption can be defined as the process of changing data into a form that is unintelligible by unauthorized persons for the purpose of ensuring the security or confidentiality of the data and privacy of the individuals transmitting them.⁶ A common understanding of commercial encryption is its use as a tool to ensure that communications are accessible only by authorized persons, but other uses, such as verifying authenticity and preventing the undetected change of information content, are no less important. The military and intelligence community also use encryption to safeguard their communications, but this other use of encryption comprises only a small fraction of its total use today. This paper focuses only on the use, purpose and value of commercial encryption,

which, as explained below, is critical to reaping the benefits from the information economy.

The use of encryption in everyday commercial activities is widespread. Encryption technology is included in, for example, ATMs and smart cards to validate transactions; mobile phones and other wireless devices to ensure the privacy of communications; and medical applications to protect sensitive personal information (see Box 1 below). The purpose of encryption in these commercial applications is to protect against unauthorized or criminal activity, not to hide communication from state actors. Many of the applications involve some form of communication between a variety of devices, as encryption is needed both to verify identity and secure the information content. This means that as more and more devices are connected with each other (the so-called “internet of things”), more and more devices will include encryption technology.⁷

Encryption, like so many other modern-day technologies, relies on semiconductors. Whether conducted through software or specialized hardware, encryption requires data processing and storage, which in turn requires the use of semiconductor chips. Thus, in practical terms, the two are inseparable; anything with encryption will need a semiconductor chip, and the odds of anything with a chip having encryption are high and getting higher.

Box 1: Everyday products that use encryption⁸

Products that include encryption technology are so prevalent that an ordinary citizen would be unlikely to spend a day without using some of them. The following are examples:

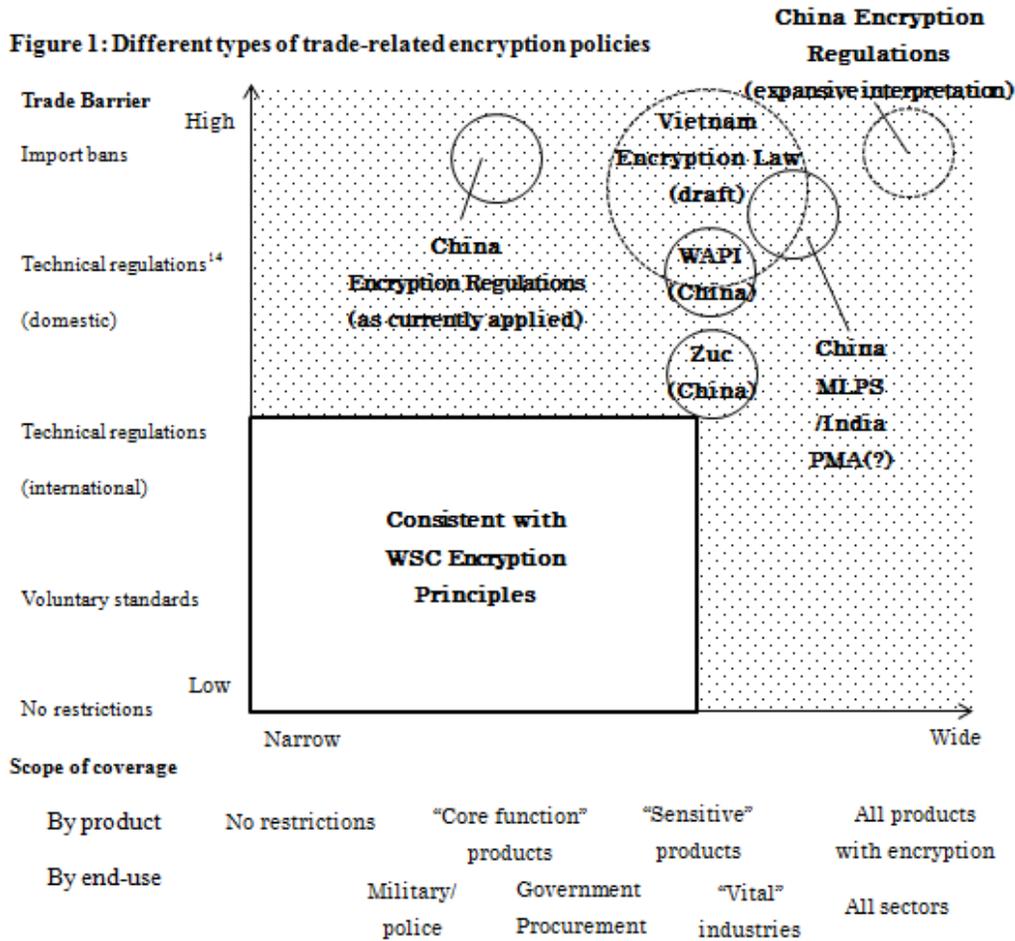
ATM machines	Hard disks	Online voting	Smartphones
Bluetooth headsets	Healthcare applications	Operating systems	Tablets
CD players	(e.g. wireless health monitoring devices)	Password management software	USB/Flash drives
Databases	In-flight (airplane) entertainment systems	Passports	Utility meters
Desktop computers	Mass transit control systems (trains, subways)	Photocopiers	Video on a mobile device
Digital cameras	Modems	Printers	Voice recognition software
Digital signatures	MP3 files	Routers	Voice over IP (VOIP) phones
DVD players	MP3 players	Scanners	Voice/video email
E-mail	Mobile phones	Semiconductors/microprocessors	Wireless networking
E-readers (e-books)	Netbook computers	Servers	Wireless watches
Fax machines	Notebook computers	Set-top boxes (e.g. for cable TV)	Word processing software
File backup software	Online banking	Small Cell/Femto Cell extender devices	World Wide Web (https://) (“https://”)
Financial systems	Online chat	Smart cards	
Game consoles	Online shopping		
Gaming software			
Global positioning systems (GPS)			

Traditionally, implementation through software has been seen as less expensive but slower.⁹ More recently, given both new security threats and widespread diffusion of relevant technology, there appears to be a trend to increase hardware-based implementation, although the best approach continues to depend on the circumstances in which encryption is used.¹⁰

A FRAMEWORK FOR CATEGORIZING ENCRYPTION POLICIES

Given its historical links to military use, encryption has in the past been regulated to a certain extent. For instance, the U.S. government classified encryption products as “munitions” and subjected them to strict export controls until the 1990s. With the development of easy-to-use encryption technology and the spread of the internet and e-commerce, which dramatically increased demand for encryption, such restrictions came to be seen as causing more harm than benefit. The Clinton Administration dropped plans to impose unwieldy regulations on such products and removed most restrictions on exports, leading to a widespread trend towards similar deregulation elsewhere.¹¹ The United States has no restrictions on the importation or domestic commercial use of foreign encryption. A minority of countries have, however, persisted in imposing strict restrictions on the commercial use of encryption, especially foreign encryption.¹²

Where encryption policies today pose obstacles to trade, they can be categorized based on two broad characteristics: the type of trade barrier adopted by the government, and the scope of its application.¹³ The scope of application in turn can be determined in one of two ways: by focusing on products, and by focusing on the type of end-uses. The tables in the annex provide an overview of each of these elements; Figure 1 presents a simplified visual representation.



14

TRADE RELATED ENCRYPTION POLICY: EXAMPLES OF BEST AND ACTUAL PRACTICES

Best Practices

An example of current regional “best practices” in this area are the Encryption Principles developed by the World Semiconductor Council (WSC) and endorsed at the Government and Authorities Meeting on Semiconductors (GAMS) since 2010.¹⁵ These principles “make it clear that generally there should be no regulation of cryptographic capabilities in widely available products used in the domestic commercial market,”¹⁶ and also provides recommendations regarding the regulations that might be put in place in “narrow and justifiable circumstances” to minimize distortions of trade. The OECD Guidelines for Cryptography Policies adopted in 1997,¹⁷ while somewhat dated, also underline the importance of trustworthy cryptographic methods being selected through market competition, as well as the need to balance legitimate law enforcement activities with rights to privacy.

China's WAPI Standard¹⁸

WAPI was a wireless networking standard developed in China in 2003, which claimed to provide better security than the prevailing international Wi-Fi standard through the use of proprietary Chinese encryption technology. Trade tensions developed when China announced that wireless networking systems in certain technology products that were sold inside China would have to comply with this standard, which thus became a mandate.

Compliance with the WAPI standard meant incorporating encryption technology whose specifications were unclear into computers, routers and certain other high-tech products that were Wi-Fi capable, which would have required licensing from Chinese companies. This sparked a backlash from the United States, Japan and EU.

Ultimately, the dispute was resolved when China agreed not to make compliance mandatory; China also attempted, but failed, to have WAPI recognized as an international standard.

Vietnam's Proposed Encryption Rules

In May 2013, Vietnam presented its new Draft Law on Information Security.¹⁹ This draft law contains provisions similar to China's Administration of Commercial Encryption Regulations, and in its current form can be considered a very broad restriction on the import and use of encryption products. Like the Chinese regulations, this draft law bans the import and use of foreign encryption products, with only a few exceptions for entities such as foreign embassies. There is also no clear delineation regarding what is and is not an encryption product. While it is possible that the authorities have in mind a provision limiting the application to products whose core purpose is to provide encryption, there are no such stipulations in the draft law itself.²⁰

The U.S. semiconductor industry has highlighted concerns with this proposed regulation, in particular with regard to various articles that constrain "civic" cryptography, which could place excessive burdens on trade in commercial ICT products.²¹ It has also been pointed out that such restrictions would appear to be inconsistent with commitments made by Vietnam at the time of accession to the WTO.²² At the time of writing, it remains to be seen whether the draft law will be amended to take these concerns into account before it is passed.

India's Proposed Preferential Market Access (PMA) Policy

India's Policy for Providing Preference to Domestically Manufactured Electronic Goods (PMA Policy), originally outlined in February 2012, is an example of a broad government "cyber security" initiative that includes an element of regulating encryption in the private sector.²³

The policy aims to impose domestic preferences in the procurement of electronic products by both the government

and by the private sector in cases “which have security implications for the country”.²⁴ A list of covered products has been announced for government procurement, and a similar draft list prepared for private companies considered “Government Licensee[s],” a phrase which appears to refer to telecommunications carriers in particular.²⁵ Both of these lists include “Encryption/UTM platforms,” as well as numerous other electronic products (mostly communications devices), so that companies developing these products could be forced to choose between moving some activities to India and giving up selling to these end users.²⁶

Opposition to this policy by the United States and others prompted the Indian government to review the entire policy, and to suspend moves to apply it to the private sector, in July 2013.²⁷ Since the policy was not, however, abolished completely, further details regarding a revised policy were being awaited at the time of writing.

Russia’s Import Licensing Requirements for Products with Encryption

In the past, Russia has required extensive licensing requirements of commercial encryption products.²⁸ As part of its WTO accession commitments, which became legally binding in August 2012, Russia has applied an “interim system” that divides imports into three goods; one group can be imported “without any formalities related to encryption,” another would require “a one-time notification requirement,” and a third “would be subject to an expert evaluation and require an import licence.”²⁹

Items included in the first two categories include, in theory, goods with relatively unsophisticated encryption algorithms, “mass market goods” and other items that are not controlled under the Wassenaar Arrangement on export controls.³⁰ This means, however, that commercial ICT goods with encryption algorithms considered very weak in the United States could still easily require a license for importation into Russia.³¹ Additionally, the actual determination of whether a product is a “mass market good” etc. is made by Russian authorities, and even goods that should not require licences for importation have in practice been found to need them, because necessary changes to domestic regulations have not been made.³²

EVALUATING THE IMPACT OF ENCRYPTION POLICIES AND RELEVANT TRADE RULES

What kind of impact on trade could various encryption policies have? The answer depends on the exact nature of the policy, and which country or group of countries is engaging in it. Below, I will note some countries that have shown an inclination to adopt restrictive policies in the past, before attempting to assess the impact of new policies being introduced in those countries.

Countries that may be Inclined to Adopt More Restrictive Trade Policies

Among the current negotiating parties of the TPP, the aforementioned draft encryption law in Vietnam stands out as the only attempt of note to place restrictions on the import and use of encryption technology (although others, including the United States, have some restrictions regarding exports).

Of major economies outside of the TPP, the three that have shown the greatest interest in regulating encryption technology are China, India and Russia.³³ China, as already mentioned, has a broad law regulating encryption, and on several occasions has mandated, or threatened to mandate, the use of domestically developed encryption algorithms. India also has IT laws on the books that in theory, forbids the use of strong encryption algorithms, though they seem to have been rarely enforced in practice. Russia has also placed limits on imports of encryption technologies.

The possibility that these countries will adopt stricter restrictions in the future is unfortunately not negligible. This could come about through several different routes.

One is a straightforward introduction or tightening of broad encryption restrictions, such as the draft Vietnamese law or a change in the “core function” test in China to widen the scope of restricted encryption products. Another is the continued adoption of more stringent cyber security regimes for “critical” industries, such as through China’s Multi Level Protection Scheme (MLPS) or India’s draft PMA regulations, which may reference domestic encryption requirements.³⁴ Either way, such developments will be underpinned by the increased sophistication of domestic industries, which will make it feasible and more attractive to require encryption related technology to be tested or sourced within the country (often not yet true today).³⁵

Affected Trade Volumes

Tables 1 and 2 below provide some rough estimates regarding the volumes of trade affected by such encryption policies, based on publicly available trade data and a definition of “ICT products” adopted by the OECD in 2008. For instance, in 2011 (the latest full year available), Vietnam imported \$3.7 billion worth of semiconductors. In the broader category of ICT products, imports totaled \$10.9 billion. What proportion of this would be affected by encryption

regulations? It is difficult to answer this question, even if we adopt the (very broad) definition that any device that includes encryption, or is needed to make encryption function, can be considered an encryption product.

Table 1: Rough estimates of semiconductor trade affected by encryption policies³⁶

Country	Import values	Proportion affected	Affected imports
Vietnam	\$3.7 billion	90%+	\$3.3 billion
China	\$188.4 billion		\$169.6 billion
India	\$3.4 billion		\$3.1 billion
Russia	\$0.7 billion		\$0.6 billion

Table 2: Rough estimates of ICT product trade affected by encryption policies³⁷

Country	Import values	Proportion affected	Affected imports
Vietnam	\$10.9 billion	50-90%	Up to \$9.8 billion
China	\$266.0 billion		Up to \$239.4 billion
India	\$25.9 billion		Up to \$23.3 billion
Russia	\$23.7 billion		Up to \$21.3 billion

Looking at semiconductors, in addition to chips whose specific function is to provide encryption, general-purpose microprocessors would be included under this definition. Other types of chips, such as memory chips or discrettes and analog chips, may not themselves be used to provide encryption functions, but in many cases would still be intended for use as part of a system that contains encryption functions in some way. Given that roughly 90% of the import value of semiconductors to Vietnam consists of ICs, one very rough estimate might be to say that at least 90% of semiconductor imports would be affected by encryption regulations.³⁸

Coming up with a similar estimate for ICT products is even more challenging. A look at the products covered in the list of ICT products that are accounted for in the figures provided above (computers and peripheral equipment, communications equipment, etc.) suggests that the majority of products are likely to contain some form of encryption within them, or be a part of a product that contains encryption.³⁹ Thus, somewhere in the range of 50-90% of non-semiconductor ICT products might be similarly affected.

Based on these assumptions, we could say that semiconductor imports worth \$3.3 billion, and ICT imports worth \$9.8 billion, might be rough estimates of trade affected by encryption regulations in Vietnam alone; similar estimates have been provided for the other three countries above.

It is worth keeping in mind that these trade volumes are likely to increase considerably in the future. For instance, in the

three-year period from 2008 to 2011, Vietnamese semiconductor imports quadrupled (from \$0.9 billion to \$3.6 billion), while total ICT product imports more than doubled (from \$5.1 billion to \$10.9 billion). Thus, while it may be too simplistic to extrapolate recent growth rates indefinitely in the future, the figures mentioned above could easily be several times larger in the near future.

Associated Costs

What would be the associated costs for the semiconductor industry to adapt to extra trade restrictions? Again, the details will depend on the exact measures, and in some circumstances adaptation may not be possible (e.g., where there is an outright ban on foreign encryption technology and domestic technology is not compatible with the ICT product). Where mitigating measures can be taken, there are a variety of costs that need to be kept in mind, as outlined below. Upfront costs to modify and/or certify products depends on specific requirements, but could potentially include expensive redesigns or abandonment of certain markets altogether; time delays due to compliance with burdensome conformity assessments which will inevitably be expensive, and could serve as a trade barrier that negates the benefits of tariff elimination; and requirements to disclose intellectual property during the assessment process, which introduce the risk of either crippling damage to business interests or forcing companies to forego market opportunities.

Costs to modify and/or certify products

The draft Vietnamese law, in addition to banning the general importation and use of foreign encryption products, also mentions technical regulations and standards relating to information security, as well as conformity assessments to certify compliance.⁴⁰ It is therefore possible that some or even most ICT imports would be allowed subject to suitable testing, or perhaps some form of non-cumbersome modification. At this level of generality, however, it is impossible to evaluate how large the cost of such adaptations might be.

“Past research has shown that... domestic standards tend to result in higher costs and lower trade volumes compared to international standards.”

Even if an extra requirement by one country does not cause much increase in costs, it could touch off similar (but incompatible) requirements by other countries. This would force manufacturers to make different versions of the same product for such countries, losing benefits from large-scale production and possibly causing interoperability issues; some have termed this “fracturing the global digital infrastructure.”⁴¹ Past research has shown that, especially for sophisticated manufactured goods such as electronic products, domestic standards tend to result in higher costs and lower trade volumes compared to international standards.⁴²

Time delay costs

Even if little modification is required for products to avoid an importation ban, the certification process will almost certainly consume extra time. Given the importance of timely shipments in complicated electronics supply chains that make up dynamic and highly competitive industries, such delays themselves would impose real costs on companies, easily equivalent to tariffs of several percentage points.⁴³

“Delays themselves would impose real costs on companies, easily equivalent to tariffs of several percentage points.”

Potential costs from unauthorized disclosure of intellectual property

Another potential cost arising from an attempt to comply with unique technical regulations is the possibility of damage to intellectual property arising from conformity assessment procedures. Again, Vietnam’s draft law stipulates that such assessments would be conducted by designated organizations, with the possibility of mutual recognition where treaties are applicable.⁴⁴ Given that Vietnam is not a signatory to, for instance, the Common Criteria Recognition Arrangement, which calls for mutual recognition of certification results, it would seem that assessment by a Vietnamese organization is likely. If such organizations themselves do not maintain a high standard of information security, and if the provision of sensitive intellectual property is required as part of the conformity assessment procedure, there is the possibility that leaks to competitors, whether intended or otherwise, could occur, thus imposing a further cost related to the regulations.⁴⁵

WHERE ARE THE GAPS IN EXISTING TRADE RULES, AND HOW WOULD THE TPP HELP PLUG THEM?

There are existing trade rules that could constrain some of the encryption policies explained above, most notably, the WTO Agreements (principally the GATT and TBT Agreement). One could make the case that many restrictions on the import and use of encryption products would seem to run afoul of the non-discrimination provisions in these agreements; unfortunately, there are also reasons to believe that bringing a WTO case would not provide an easy solution. While a thorough examination of the legal issues is beyond the scope of this paper, I will provide a brief sketch of these existing disciplines.

In terms of restrictions on use and import, GATT Article XI (General Elimination of Quantitative Restrictions) bans “prohibitions or restrictions other than duties, taxes or other charges” on imports; Article III (National Treatment on Internal Taxation and Regulation), paragraphs 1 and 4 provide for national treatment regarding “laws, regulations and requirements affecting the internal sale, offering for sale, purchase, transportation, distribution or use of products.” Regarding technical regulations, Articles 2.1 of the TBT Agreement also provides for national treatment, while Article 2.2

states that “technical regulations shall not be more trade-restrictive than necessary to fulfil a legitimate objective, taking account of the risks non-fulfilment would create;” Article 2.4 mandates that where international standards exist, WTO members use them “as a basis for their technical regulations” unless there are special circumstances that render such standards ineffective or inappropriate.

There are, however, exceptions to the above rules. The one most likely to be invoked with regard to encryption regulations is the (national/essential) security exception, which is articulated in GATT Article XXI and Article 2.2 of the TBT Agreement; within the bounds of these provisions, WTO members have the right to deviate from the “normal” rules. It is worthwhile, however, to note two points here. Firstly, the scope of these exceptions are not unlimited; for instance, encryption products would have to be classified in the category of “arms, ammunition and implements of war,” and trade restrictions deemed “necessary for the protection of [the WTO Member’s] essential security interests,” for the GATT Article XXI exception to apply. Secondly, such security exceptions have in practice rarely been invoked in the past.

“Adopting clearer rules that deal squarely with encryption issues could provide substantial benefits, by providing concrete assurances that new, more restrictive encryption policies will not be adopted in the future.”

At the same time, it is also true that once the use of such an exception is claimed by a sovereign state, it is difficult for other nations or international institutions to dismiss such a claim unless there is some glaring flaw in the argument. In other words, although there are existing disciplines that should be relevant to trade restrictions regarding encryption products, there remains a certain degree of ambiguity about what sort of measures are allowed and what are not.

One way to reduce such ambiguities is to challenge measures on a case-by-case basis through the appropriate dispute settlement mechanism; the drawback to this approach is that clarity would be provided only in a piecemeal manner, and only after measures are implemented and have already caused harm. This is why adopting clearer rules that deal squarely with encryption issues could provide substantial benefits, by providing concrete assurances that new, more restrictive encryption policies will not be adopted in the future.

Currently, the SIA and others have called on TPP countries to include rules that:

- specify that the import, use, and sale of products containing encryption in commercial markets should be largely unrestricted;
- in narrow circumstances where regulation regarding the domestic use of encryption may be justified (e.g., certain government or military uses), encourage a flexible, global approach.⁴⁶

While the exact language to be included in a completed TPP agreement remains to be seen, rules along these lines would fit the bill for reducing the grey area surrounding encryption.

BEYOND A SUCCESSFUL TPP AGREEMENT- EXPANDING THE REACH OF NEW RULES

One final question that will need to be addressed in the future is the applicability of trade rules, such as those being discussed in the TPP negotiations, regarding encryption. A prerequisite for any new international trade rule to formally apply to a certain country is that that country must agree to be bound by such rules. Of the countries mentioned in the examples given above, Vietnam is a member of the TPP negotiations, but China, India and Russia are not. Thus, it is important to spell out the reasons why strong encryption disciplines in the TPP would encourage non-TPP member countries to avoid restrictive policies.

Firstly, there is the obvious possibility of expanding the TPP to include more countries. The TPP has been recognized by APEC leaders as providing a basis for a Free Trade Area of the Asia-Pacific.⁴⁷ Both China and Russia are APEC members, although India is not, and while it would be too optimistic to expect these countries to join the TPP in the near future, it remains an option to pursue in the medium to long term.

“It is important to spell out the reasons why strong encryption disciplines in the TPP would encourage non-TPP member countries to avoid restrictive policies.”

Secondly, at an informal level, rules adopted by a large number of major trading nations will affect the expectations and could also influence the behavior of private actors and other states, even if they are not legally enforceable outside of the TPP member countries. If such rules are seen to be successful best practices, companies and individuals will push for similar policies to be implemented, which could lead to a de facto trend towards convergence in this area.

Thirdly, a set of suitably articulated rules in the TPP would serve as a basis for similar rules to be adopted in other contexts. There have already been suggestions that similar rules should be adopted in the U.S.-EU free trade talks (Transatlantic Trade and Investment Partnership (TTIP)), from industries on both sides.⁴⁸ Given that the authorities have also endorsed the WSC Encryption Principles, there seems to be a good chance of this happening. Once it does, it would become likely that similar provisions would be adopted in any new FTAs negotiated by the United States, EU or Japan. The possibility of adopting similar rules at the multilateral level (WTO), or through other plurilateral arrangements (for example, APEC or OECD) would also be greatly enhanced.

While none of these possibilities are guaranteed, it would be reasonable to say that a good set of rules in the TPP should serve as a launch pad for expanding the reach of such rules to the countries where it is most needed.

CONCLUSION

While encryption is not “new,” its use in everyday life has become dramatically more common since the rise of the internet, the exponential increase in e-commerce and the proliferation of digital devices. This trend looks set to continue for the foreseeable future. As a practical matter, semiconductors are inseparable from encryption; where there are semiconductors, there will be some form of encryption taking place in the hardware integrated circuits as well as in corresponding software, and vice versa. It is therefore in the interest of the semiconductor industry to ensure that rules governing the use and trade of encryption products do not unfairly impede the trade of semiconductors, or more broadly, ICT products that depend on them.

Rough calculations suggest that the adoption of restrictive encryption policies could easily affect trade in such products on the scale of billions, if not tens or even hundreds of billions, of dollars. Some relevant disciplines do already exist in international trade law, but there remain sufficient unresolved questions to cause uncertainty about future rule changes and the possibility of trade disputes in the future.

“...the adoption of restrictive encryption policies could easily affect trade in such products on the scale of billions, if not tens or even hundreds of billions, of dollars.”

It would thus be enormously beneficial to set out specific rules within a cutting-edge trade agreement, the TPP, to provide assurances to businesses that unwanted major changes in the commercial environment will not occur. These rules would, in the short term, apply only to the 12 current members of the TPP negotiations, but in the mid to long term, could serve as a basis for similar rules encompassing trade between all major regions of the globe.

ANNEX

Table A: Types of encryption trade barriers

Trade barrier	Explanation	Examples
Ban on foreign encryption products	The most extreme form of import restriction simply blocks all imports of foreign encryption products.	Encryption regulations in China, Vietnam (draft)
Requirement to adopt specific standards/ disclosure requirements	Countries may require that encryption products meet some standard in order to be authorized for import and domestic use.	
Domestic standards / disclosure requirements	Can present a high hurdle if unique requirements or testing procedures need to be met; risk of damage to intellectual property if disclosure of sensitive business information (e.g. source code) is required.	WAPI, MLPS, Trusted Computing Module (TCM), Chinese Compulsory Certification (CCC), Indian PMA
International standards ⁴⁹ / disclosure requirement	May pose less of a problem, but could still present challenges if they are misused, or are implemented in unorthodox ways.	Zuc, Wi-fi
Voluntary adoption of standards	Can be problematic if the government pressures sources of demand (e.g. telecoms companies) to refuse to accept products that do not satisfy “voluntary” standards.	Zuc, Trusted Platform Module (TPM)
(Tariffs)	Theoretically possible, but does not seem to have been adopted so far.	

High
↑
↓
Low

Table B: Scope of regulated products

	Regulated product	Explanation	Examples
Broad   Narrow	Any product including encryption technology	Any product with electronics inside could potentially include encryption in it, especially if it is designed to communicate with other devices.	Encryption regulations in China, Vietnam (if applied expansively)
	Products including encryption technology and deemed “sensitive”	One way in which the scope of “encryption products” can be narrowed is by specifying a certain category of products that both use encryption technology and are deemed “sensitive,” e.g. certain types of telecommunications equipment (mobile phones and other wireless devices, routers etc.).	WAPI, Zuc, CCC
	Products with encryption as “core function”	A product that includes encryption technology would only be regulated if encryption was a “core function”: i.e. encryption software would be regulated, but word processing software that included encryption functions would not.	Encryption regulations in China (as currently applied through administrative guidance)

Table C: Scope of regulated end-users

Regulated end-use	Explanation	Examples
All commercial activities	A broad application of restrictions on imports with narrow exceptions only for, for example, foreign government entities or foreign companies that require such products to uphold internal procedures.	Encryption regulations in China, Vietnam
“Vital” industries	Another approach is to specify some industries that deal with “vital” public infrastructure (energy, transport, etc.) and require those industries to adhere to certain encryption-related standards. In this case, the requirements relating to encryption are likely to be merely one facet of broader cyber security regulations.	MLPS, Indian PMA
General government	Restrictions could apply only to procurement by the public sector. The actual scope of the “public sector” (for instance, whether it includes state owned enterprises) can determine how broad the application actually is.	WAPI, CCC
National security apparatus	Within the government sector, certain entities, such as the military and other national security apparatus, may have special requirements that call for special scrutiny or avoidance of foreign encryption products.	

Broad




Narrow

ENDNOTES

¹ Research Fellow (Summer 2013), Semiconductor Industry Association (SIA); MPP Candidate, Harvard Kennedy School. Opinions expressed in this paper are the author's own and do not necessarily reflect those of the organizations with which the author is associated. In addition to all of the interviewees listed at the end of this paper, the author would like to thank Daryl Hatano of ON Semiconductor, and Stephanie Flores, Devi Keller, Daniel Rosso, Ian Steff and Falan Yinug of SIA for their help and advice.

² USTR (2013a).

³ SIA (2013a, p.2).

⁴ For instance, WSC (2013) both notes the success of the ITA in the past and requests updates in line with technological progress.

⁵ SIA (2013a).

⁶ For examples of definitions, see NIST (2013), OECD (1997) and WSC (2013) (Annex I).

⁷ With the increased use of electronics, encryption is needed for communication within a single "product" as well; for an intriguing example involving tire pressure monitors, see Clayton (2010).

⁸ Based on an illustrative list prepared by SIA, Information Technology Industry Council (ITI), and Alliance for Network Security (ANS).

⁹ NIST (2005, p.29).

¹⁰ For arguments in favor of a hardware-based information security platform (albeit sponsored by an interested party), see Shpantzer (2013), which also cites stated preferences by NIST for hardware-based solutions in some applications.

¹¹ Swire & Ahmad (2012, pp. 433-441), provides an overview of these developments. The Electronic Privacy Information Center (EPIC) conducted annual surveys of global encryption policies from 1998-2000, the last of which declared: "Most countries in the world today impose no restrictions on the use of cryptography. In the vast majority of countries, cryptography may be freely used, manufactured, and sold without restriction." (EPIC (2000)).

¹² For examples, see policies described later in this paper.

¹³ Here, I deal exclusively with restrictions on the import and domestic use of encryption, although export restrictions (mostly in a limited form) are still in place in various countries.

¹⁴ In the TWO Technical Barriers to trade (TBT) Agreement, "technical regulation" refers to a rule with which compliance is mandatory, whereas compliance with a "standard" is voluntary. See Annex 1 of the TBT Agreement.

¹⁵ WSC (2013) Annex I. The WSC is made up of the semiconductor industry associations from China, Chinese Taipei, the EU, Japan, Korea and the United States.

¹⁶ Ibid.

¹⁷ OECD (1997)

¹⁸ There are numerous sources that describe the WAPI case. See, e.g. Kennedy (2006, pp.48-56); USITC (2010, pp. 5-15-5-16); Swire and Ahmad (2012, p. 448).

¹⁹ Socialist Republic of Vietnam, Draft Law on Information Security (May 22, 2013).

²⁰ This has been the approach taken in China, through the so-called "core function" test; unfortunately, this rule is in the form of administrative guidance and not enshrined in law.

²¹ SIA (2013b).

²² Ibid., p.4.

²³ Ministry of Communications and Information Technology of India, Department of Information Technology (2012).

²⁴ Ibid.

²⁵ For the draft lists, see Ministry of Communications and Information Technology of India, Department of Telecommunications (2012/2013).

²⁶ The expansive nature of the list did not fit well with the stated aim of "security" for the whole policy; for instance, USTR (2013b,

p.23) notes that “initial draft lists of these products appear to cover an unduly broad range of electronic products so as to call into question whether security concerns, rather than industrial policy, are the primary motivation for imposing such requirements on private firms.”

²⁷ Hoffman (2013) outlines U.S. IT industry concerns regarding this issue. The Indian government’s decision is outlined in Office of the Prime Minister of India (2013).

²⁸ WTO (2011), paragraph 472 (statement by the Russian representative).

²⁹ Ibid., paragraph 473 (statement by the Russian representative); US&FCS(2013, p.100).

³⁰ WTO (2011), paragraphs 473-480.

³¹ For instance, with symmetric algorithms, only those with key lengths up to 56 bits are included in this definition; a paper published in 1996 noted that “the U.S. Data Encryption Standard with 56-bit keys is increasingly inadequate.” (Blaze et al. (1996))

³² U.S. & Foreign Commercial Service (2013, p.100) notes that “[the] “mass market” category should help to facilitate access for U.S. exports to the Russian market, but implementation will need to be observed closely, as Russia will maintain the authority to define what constitutes a “mass market” good.” USTR (2013b, p.315) notes that “As part of its WTO accession, Russia committed to reform its import licensing regime for such encryption products... However, the necessary amendments to the CU regulations governing the import licensing of these products still have not been made, inhibiting trade in these products.”

³³ Swire and Ahmad (2012, pp. 441-449) provide a summary of these countries’ policies, especially India and China.

³⁴ Ernst (2011, pp.33-39) describes the MPLS scheme in some detail.

³⁵ An industry expert noted that, for instance, restrictions on imports of semiconductors into China may become more likely if China’s own semiconductor industry becomes more developed.

³⁶ “Semiconductor trade” refers to UN Comtrade trade data for HS codes 8541 & 8542; data 2011 for Vietnam, 2012 for China, India and Russia.

³⁷ “ICT product trade” refers to UN Comtrade trade data based on definition in OECD (2009), with concordance to HS 2007 categories provided in OECD (2010); data 2011 for Vietnam, 2012 for China, India and Russia.

³⁸ In interviews, one U.S. semiconductor company explained that 100% of chips designed there included encryption functions; another noted that there may be a small minority of exceptions.

³⁹ For the full list, see OECD (2009) (Table 3), and OECD (2010) (Annex Table).

⁴⁰ Socialist Republic of Vietnam, Draft Law on Information Security (May 22, 2013), Articles 33-35.

⁴¹ WSC (2013) (Annex I).

⁴² Portugal-Perez, Reyes and Wilson (2010) examine the impact of different kinds of standards on imports of electronic products into the EU; their econometric analysis “confirms the importance of international harmonisation of standards on the commercialisation of more complex goods, such as electronics, as well as on their production and consumption” (p.1895). See also Ezell and Atkinson (2010, pp.84-90); OECD (2000); USITC (1998).

⁴³ For instance, Hummels and Schaur (2012) conclude from a study of the willingness of businesses to pay for different options to transport goods that “each day in transit is equivalent to an ad-valorem tariff of 0.6 to 2.3 percent and that the most time-sensitive trade flows are those involving parts and components trade” (Abstract).

⁴⁴ Socialist Republic of Vietnam, Draft Law on Information Security (May 22, 2013), Article 35.

⁴⁵ A point raised with regard to conformity assessments in general by Ezell and Atkinson (2010, pp.88-90).

⁴⁶ Presentation to TPP member governments by ITI, SIA, ANS.

⁴⁷ “ We believe that an FTAAP should be pursued as a comprehensive free trade agreement by developing and building on ongoing regional undertakings, such as ASEAN+3, ASEAN+6, and the Trans-Pacific Partnership, among others.” (APEC (2010))

⁴⁸ For example, see SIA (2013c, p.4-6) and ESIA (2013, p.2-3).

⁴⁹ Standards adopted in international bodies with open participation of stakeholders from different countries.

REFERENCES

- Asia Pacific Economic Cooperation. (2010, November 14). *2010 Leaders' Declaration- Pathways to FTAAP*.
- Blaze, M. et al. (1996). *Minimal Key Lengths for Symmetric Ciphers to Provide Adequate Commercial Security*. Retrieved from <http://www.schneier.com/paper-keylength.pdf>.
- Clayton, M. (2010, August 13.) "Scientists hack into cars' computers -- control brakes, engine". *Christian Science Monitor*. Retrieved from <http://www.csmonitor.com/USA/2010/0813/Scientists-hack-into-cars-computers-control-brakes-engine>.
- Electronic Privacy Information Center. (2000). *Cryptography and Liberty 2000: An International Survey of Encryption Policy*. Washington, DC: Electronic Privacy Information Center.
- Ernst, D. (2011). *Indigenous Innovation and Globalization: The Challenge for China's Standardization Strategy*. La Jolla, CA: UC Institute on Global Conflict and Cooperation; Honolulu: East-West Center.
- European Semiconductor Industry Association. (2013, June 18). *ESIA Position EU-U.S. Transatlantic Trade and Investment Partnership (TTIP)* [Public Comment]. Retrieved from <https://www.eeca.eu/data/File/ESIA%20news/2013/June/ESIA%20Position%20TTIP.pdf>.
- Ezell, S.J. and Atkinson, R.D. (2010). *The Good, The Bad, and The Ugly (and The Self-Destructive) of Innovation Policy: A Policymaker's Guide to Crafting Effective Innovation Policy*. The Information Technology and Innovation Foundation.
- Hoffman, R. (2013, June 27). Testimony at Subcommittee on Commerce, Manufacturing, and Trade, Committee on Energy and Commerce, U.S. House of Representatives. Retrieved from <http://democrats.energycommerce.house.gov/sites/default/files/documents/Testimony-Hoffman-CMT-Trade-Barriers-India-US-2013-6-27.pdf>.
- Hummels, D. and Schaur, G. (2012). *Time as a Trade Barrier*. NBER Working Paper 17758.
- Kennedy, S. (2006). "The Political Economy of Standards Coalitions: Explaining China's Involvement in High-Tech Standards Wars". *Asia Policy*, No.2 (July 2006), 41–62.
- Ministry of Communications and Information Technology of India, Department of Information Technology. (2012, February 10). *Subject: Preference to domestically manufactured electronic goods in procurement due to security considerations and in Government procurement* [Notification]. No. 8(78)/2010-IPHW. *Gazette of India*, 15 February 2012, 1-14.
- Ministry of Communications and Information Technology of India, Department of Telecommunications. (2012, October 5). *Subject: Policy for Preference to domestically manufactured telecom products in procurement due to security considerations and in Government procurement - Notifying Telecom Products for Government Procurement in furtherance of the Policy* [Notification]. No. 18-07/2010-IP. Retrieved from <http://dot.gov.in/sites/default/files/5-10-12.PDF>.
- Ministry of Communications and Information Technology of India, Department of Telecommunications. (2013, January 17). *Draft List of Security Sensitive Telecom Products for Preferential Market Access (PMA) by Government Licensee - for stakeholders' consultation*. Retrieved from <http://www.dot.gov.in/sites/default/files/Draft%20List%20of%20Security%20Sensitive%20Telecom%20Products%20for%20PMA%20by%20Govt%20Licensee-consultation%20dated17-01-2013.pdf>.
- National Institute of Science and Technology. (2005). *Guideline for Implementing Cryptography In the Federal Government*. NIST Special Publication 800-21 [Second Edition]. Retrieved from http://csrc.nist.gov/publications/nistpubs/800-21-1/sp800-21-1_Dec2005.pdf.
- National Institute of Science and Technology (2013). *Glossary of Key Information Security Terms*. NISTIR 7298 Revision 2. Retrieved from <http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf>.

- Office of the Prime Minister of India. (2013, July 8). *PMA Policy in Private Sector to be reviewed, notifications kept in abeyance* [Press release]. Retrieved from <http://pmindia.nic.in/press-details.php?nodeid=1660>.
- Organisation for Economic Co-operation and Development. (1997, March 27). *Recommendation of the Council concerning Guidelines for Cryptography Policy*. C(97)62/FINAL.
- Organisation for Economic Co-operation and Development. (2000). *An Assessment of the Costs for International Trade in Meeting Regulatory Requirements*. TD/TC/WP(99)8/FINAL.
- Organisation for Economic Co-operation and Development. (2009). "Information Economy Product Definitions Based on the Central Product Classification (version 2)". *OECD Digital Economy Papers*, No. 158, OECD Publishing. <http://dx.doi.org/10.1787/222222056845>.
- Organisation for Co-operation and Economic Development. (2010). *Measuring Trends in ICT Trade: From HS2002 to HS2007*. DSTI/ICCP/IIS(2010)5/FINAL.
- Portugal-Perez, A., Reyes, J-D., and Wilson, J.S. (2010). "Beyond the Information Technology Agreement: Harmonisation of Standards and Trade in Electronics" *The World Economy* (2010) 1870-1897. doi: 10.1111/j.1467-9701.2010.01300.x.
- Semiconductor Industry Association. (2013a, June 9). *RE: Docket Number USTR-2013-0022, Request for Comments on Negotiating Objectives with Respect to Japan's Participation in the Proposed Trans-Pacific Partnership Trade Agreement* [Public comment]. Retrieved from http://www.semiconductors.org/clientuploads/Trade%20and%20IP/SIA_Comments_on_Japan%27s_Participation_in_TPP_FINAL.pdf.
- Semiconductor Industry Association. (2013b, June 10). *Comments Submitted RE: Draft 2.22 Law on Information Security, Issued by National Assembly, Socialist Republic of Vietnam* [Public comment]. Retrieved from <http://www.semiconductors.org/clientuploads/directory/DocumentSIA/International%20Trade%20and%20IP/SIA%20Comments%20on%20Draft%20Vietnam%20Encryption%20Regulations-%20FINAL.pdf>.
- Semiconductor Industry Association. (2013c, May 10). *RE: Docket Number USTR-2013-0019, Request for Comments for the U.S.-EU Transatlantic Trade and Investment Partnership* [Public comment]. Retrieved from <http://www.semiconductors.org/clientuploads/directory/DocumentSIA/International%20Trade%20and%20IP/Final%20SIA%20Comments%20on%20the%20TTIP-May%2010.pdf>.
- Shpantzer, G. (2013). *Implementing Hardware Roots of Trust: The Trusted Platform Module Comes of Age*. Retrieved from <http://www.trustedcomputinggroup.org/files/temp/76882F9C-1A4B-B294-D09D38B918AD23D0/SANS%20Implementing%20Hardware%20Roots%20of%20Trust.pdf>.
- Swire, P. and Ahmad, K. (2012). "Encryption and Globalization". *The Columbia Science & Technology Law Review*, 13, 416. <http://www.stlr.org/cite.cgi?volume=13&article=9>.
- United States and Foreign Commercial Service. (2013). *Doing Business in Russia: 2013 Country Commercial Guide for U.S. Companies*. Retrieved from http://buyusainfo.net/docs/x_8347046.pdf.
- United States International Trade Commission. (1998). *Global Assessment of Standards Barriers to Trade in the Information Technology Industry*. USITC Publication 3141.
- United States International Trade Commission (2010). *China: Intellectual Property Infringement, Indigenous Innovation Policies, and Frameworks for Measuring the Effects on the U.S. Economy*. USITC Publication 4199 (amended).
- United States Trade Representative. (2013a, July 25). *Statement on the 18th Round of Trans-Pacific Partnership Negotiations: TPP Negotiators Press Ahead in Malaysia, Welcome Japan's Entry* [Press release]. Retrieved from <http://www.ustr.gov/about-us/press-office/press-releases/2013/july/statement-18th-round-tpp>.
- United States Trade Representative. (2013b). *2013 National Trade Estimate Report on Foreign Trade Barriers*. Retrieved from <http://www.ustr.gov/sites/default/files/2013%20NTE.pdf>.

World Semiconductor Council. (2013, May 23). *Joint Statement of the 17th Meeting of the World Semiconductor Council (WSC)*. Retrieved from <http://www.eeca.eu/data/File/ESIA%20WSC/May%202013%20WSC%20-%20Joint%20Statement%20of%20the%2017th%20Meeting%20of%20the%20WSC%20Final%2023%20May.pdf>.

World Trade Organization. (2011, November 17). *Report of the Working Party on the Accession of the Russian Federation to the World Trade Organization*. WT/ACC/RUS/70.

LIST OF INTERVIEWS

Stephen Ezell (Senior Analyst, The Information Technology & Innovation Foundation) (July 16, 2013).

Michael Ferrantino (Office of Economics, U.S. International Trade Commission) (June 18 & June 24, 2013) [By phone].

Allan A. Friedman (Fellow, Governance Studies & Research Director, Center for Technology Innovation, Brookings Institution) (July 2, 2013) [By phone].

Danielle Kriz (Director, Global Cybersecurity Policy, Information Technology Industry Council) (June 26, 2013).

Kate Linton (Office of Industries, U.S. International Trade Commission) (June 26, 2013) [By phone].

Kazuhiko Oi (Director, Washington DC Office, Japan Electronics and Information Technology Association) (June 27, 2013).

Monique I. Rodriguez (Director, Government Affairs, Qualcomm Incorporated) (July 17, 2013).

Greg Slater (Director, Global Trade and Competition, Intel Corporation) (July 18, 2013).

Roszel Thomsen (Counsel, Alliance for Network Security) (August 5, 2013) [By phone].