1-2017

Inside the black box: Political economy of the Trans-Pacific Partnership's encryption clause

Han-wei LIU
Singapore Management University, hanweiliu@smu.edu.sg

Inside the Black Box: Political Economy of the Trans-Pacific Partnership's Encryption Clause

Han-Wei LIU*

Among other provisions of the Trans-Pacific Partnership (TPP) Agreement, a new clause on encryption technology ('Encryption Clause') is particularly noteworthy. By tracing the history of decades-long encryption control, this article underscores how this clause implicates international order. Modern encryption technology was conceived and developed during World Wars. Painted by such a war-time legacy, encryption has been treated as a 'dual-use' technology and has been subject to export control since the end of World War II via the Coordinating Committee for the Control of Multinational Trade (COCOM) and, later, the Wassenaar Arrangement. With the collapse of the Soviet Union, the Western bloc became divided on encryption policies. The US was most concerned with national security and once attempted to introduce the mandatory key escrow scheme to provide a level playing field for its high-tech industry. Resistance to the US's hard line approach towards encryption at home and abroad led the nation to relax its export controls, thereby ending Crypto War 1.0. With the rise of emerging economies, however, Crypto War 2.0 is now resurfacing, and through the Encryption Clause, the US seeks to remove trade barriers that are hostile towards products employing foreign cryptography. Yet, underlying intellectual property right (IPR)(issues and the role of intelligence units in the formation of technical standards may once again move trade negotiations into the shadows.

1 INTRODUCTION

The much-anticipated text of the Trans-Pacific Partnership (TPP) finally came to light in November 2015.[1] This landmark trade deal, reached by and among twelve countries in the Pacific Rim, would have three sets of implications for international order. Economically, the current TPP parties collectively host some 40% of

* Assistant Professor of Law, National Tsing Hua University, Taiwan. While Trump's withdrawal from the TPP essentially collapsed the deal, its provisions on encryption may nevertheless feature the future direction of managing 'codes' through international economic lawmaking. I am grateful to anonymous reviewers for valuable comments and Sylvia Lu, Jung-Ming Chang, and Yi-Ting Cheng for research assistance. This article was supported by a grant awarded by the Ministry of Science and Technology, Taiwan (105-2410-H-007-002). Usual disclaimer applies. The author can be reached at han-wei.liu@graduateinstitute.ch.

1 On 5 Nov. 2015, New Zealand was the first among others that put the full text online, which was superseded by the legally verified text released on 26 Jan. 2016. For the text of the TPP, *see* New Zealand Foreign Affairs & Trade, *Trans-Pacific Partnership: Text of the Trans-Pacific Partnership*, http://tpp.mfat.govt.nz/text (accessed 4 July 2016) [hereinafter 'TPP Agreement'].

Liu, Han-Wei. 'Inside the Black Box: Political Economy of the Trans-Pacific Partnership's Encryption Clause'. *Journal of World Trade* 51, no. 2 (2017): 309–334.

the world's population, accounting for around one-third of the global GDP.[2] Its potential economic benefits designates the mega-regional agreement as a pathway toward further economic integration amid the deadlock of the Doha Round negotiations.[3] From a regulatory perspective, the TPP is often considered a 'high-standard' and 'living' agreement for trade and investment matters for the twenty-first century.[4] Its ambitious scope turns on the long-debated question of the erosion of state sovereignty.[5] Third, and more crucially for our purpose, the TPP has geo-political implications for Sino-US relations. Its conclusion marks an important step toward the US's 'Asia Pivot' strategy.[6] By imposing new rules on trade and investment issues, Americans seek to determine acceptable behaviour in the new global economic order.[7] Certain initiatives in the context of the TPP, despite their character of economic integration, are believed to be targeted at China in geo-political terms.[8]

Among others, the disciplines on encryption technology in the TPP are one such arrangement that may have economic and geo-political implications for Sino-US relations.[9] TPP Chapter 8 incorporates a set of rules governing technical barriers regarding products using encryption technologies.[10] According to section A, Annex 8-B of the TPP Agreement, referred to hereinafter as the 'Encryption Clause,' TPP parties are prohibited from imposing technical regulations or conformity assessments as a condition of the manufacture, sale, distribution, import or

---

2 Brock R. Williams, *Trans-Pacific Partnership (TPP) Countries: Comparative Trade and Economic Analysis*, CRS Report for Congress R42344, Congressional Research service, 2 (29 Jan. 2013) http://www.fas.org/sgp/crs/row/R42344.pdf (accessed 4 July 2016).

3 Tania Voon, *Introduction: National Regulatory Autonomy and the Trans-Pacific Partnership Agreement*, in *Trade Liberalisation and International Cooperation: A Legal Analysis of the Trans-Pacific Partnership Agreement* (Tania Voon eds, Edward Elgar 2013).

4 USTR Press Releases, *Summary of the Trans-Pacific Partnership Agreement*, http://ustr.gov/about-us/policy-offices/press-office/press-releases/2015/october/summary-trans-pacific-partnership (accessed 4 July 2016).

5 The TPP contains thirty chapters, covering, among others, trade in goods, agriculture, services, intellectual property rights, textiles and apparel, rules of origins, technical barriers to trade, sanitary and phytosanitary measures, regulatory coherence, and investment. *See* e.g. USTR Press Release, *Summary of the Trans-Pacific Partnership Agreement*, http://ustr.gov/about-us/policy-offices/press-office/press-releases/2015/october/summary-trans-pacific-partnership (accessed 8 July 2016).

6 Kurt Campbell & Brian Andrews, *Explaining the US 'Pivot' to Asia*, 2 (Chatham House 2013).

7 Michael Du, *Explaining China's Tripartite Strategy: Toward the Trans-Pacific Partnership Agreement*, 18 J. Int'l Econ. L. 407, 413 (2015).

8 *See* e.g. Larry Catá Backer, *The Trans-Pacific Partnership: Japan, China, the U.S and the Emerging Shape of a New World Trade*, 13 Wash. U. Global Stud. L. Rev. 49 (2014).

9 Certain mechanisms of the TPP would arguably exclude China's participation in the TPP. For instance, it would be politically and economically problematic for China to comply with the TPP's disciplines on the state-owned enterprises (SOEs). *See* e.g. Henry Gao, *From the P4 to the TPP: Transplantation or Transformation*, in *The Trans-Pacific Partnership: A Quest for a Twenty-First-Century Trade Agreement* 79 (Cambridge University Press 2012).

10 Annex 8-B to the TPP defines the term 'encryption' as 'the conversion of data (plaintext) into a form that cannot be easily understood without subsequent re-conversion (cipher-text) through the use of a cryptographic algorithm'. *See* TPP Agreement, above n. 1, at Annex 8-B, s. A, para. 2.

use of the product to disclose the proprietary encryption technology used in their products.[11] It also bars measures that force the establishment of a partnership or that require the use or integration of a 'particular cryptographic algorithm or cipher'.

An immediate question following these new disciplines follows: Why do we need the add-ons at all? A quick look at the database of the World Trade Organization (WTO) indicates that encryption products seem to be a growing concern.[12] Russia's import licence requirements on encryption items, for instance, was a subject of debate in its accession to the WTO.[13] Likewise, WTO Members requested Kazakhstan to clarify measures requiring an activity licence to engage in the import, production, or distribution of encryption goods in negotiating the accession.[14] Of particular importance to many WTO trading partners in recent years, however, is China's measures regarding encryption technologies. In 2004, for instance, China's WAPI – a technical regulation requiring wireless local area network devices to follow a specific encryption standard for consumer use – raised an outcry both within and outside the WTO.[15] A more recent example is China's Regulation on Commercial Encryption Products and the Multi-level Protection Scheme (MLPS), which, by November 2015, had been raised fourteen times before the WTO's Technical Barriers to Trade (TBT) Committee.[16]

Unfortunately, identifying these concerns only raises more questions. On its face, the Encryption Clause seems sort of the 'TBT-Plus' mechanism that addresses new non-tariff barriers. It is not clear, however, what interests are at stake here so that countries may seek to intervene and adopt certain controversial measures? Complicating the matter is a remark from Stewart Baker, the former General

---

[11] *Ibid*., at para. 3, which prohibits the TPP parties from using technical regulations or conformity assessments as a condition of market access to force foreign companies to: '(a) transfer or provide access to a particular technology, production process, or other information (e.g., a private key or other secret parameter, algorithm specification or other design detail), that is proprietary to the manufacturer or supplier and relates to the cryptography in the product, to the Party or a person in the Party's territory; (b) partner with a person in its territory; or (c) use or integrate a particular cryptographic algorithm or cipher,' unless the manufacture, sale, distribution, import or use of the product is by or for the government of a TPP Member'.

[12] As early as the late 1990s, the WTO Secretariat noted that encryption was an Internet/e-commerce-related concern. *See* e.g. Council for Trade in Services, *Computer and Related Services: Background Note by the Secretariat*, S/C/W/45, 10 (14 July 1998); Council for Trade in Services, *International Regulatory Initiatives in Services: Background Note by Secretariat*, S/C/W/97 (1 Mar. 1999).

[13] *See* e.g. Working Party on the Accession of the Russian Federation, *Report of the Working Party on the Accession of the Russian Federation to the World Trade Organization*, WT/ACC/RUS/70, WT/MIN (11)/2, paras 218, 263–264 (17 Nov. 2011).

[14] *See* e.g. Working Party on the Accession of Kazakhstan, *Draft Report of the Working Party on the Accession of Kazakhstan: Revision*, WT/ACC/SPEC/KAZ/9/Rev. 15, paras 281–288 (11 June 2015).

[15] *See* e.g. Committee on Technical Barriers to Trade, *Specific Trade Concerns Raised*, G/TBT/GEN/74 (25 Sept. 2008).

[16] Trade Policy Review Body, *Overview of Developments in the International Trading Environment: Annual Report by the Director-General (Mid-October 2015)* 44 (17 Nov. 2015).

Counsel of the National Security Agency (NSA), who described the Encryption Clause as 'the USTR's victory over the Crypto Wars'.[17] Presumably, this clause interlinks with cybersecurity concerns. Yet, what remains unclear is the reason for the crypto wars, as well as who the losers might be, why, and, more crucially, economic and geo-political implications behind these legal norms.

Thus far, all of these issues remain largely unexplored. This article represents an effort to identify sources of controversy surrounding trade in encryption goods by unpacking the economic and political stakes underlying these new rules. Against this backdrop, this article proceeds as follows. Section 2 begins with a necessary but brief introduction to encryption and its role in the digital world. Section 3 then contextualizes the crypto wars by examining the historical developments of how such technologies had been regulated in the West. By exploring the hidden root of the information and communication technology (ICT) industry, we illustrate how domestic and international political economy played out in shaping the US's encryption policy in the post-Cold War era. Such contexts help us, on one hand, understand why the crypto war resurfaces in recent years, and on the other, reflect upon the way in which the US leverages the mega-preferential trade agreement (PTA) to deter its geo-political rivalries. Section 4 considers, more critically, how effective can the Encryption Clause bring the new crypto war to an end. Section 5 concludes.

2 DEMYSTIFYING THE PUZZLE: ENCRYPTION TECHNOLOGY AND ITS PROMISES AND PERILS

2.1 The basics of encryption technology

The practice of encrypting communications to protect secrecy has existed for centuries.[18] The secret messages allegedly used by Julius Caesar, known as 'Caesar Cipher,' to communicate with his generals during military campaigns are believed to be one of the earliest examples.[19] The Caesar Cipher disguised plaintext by replacing every letter of the original message with a letter a fixed number of places down the alphabet – 'Return to Rome', for instance, would be encoded as 'UHWXUQ WR URPH,' nonsense to the enemies without the key.[20] Centuries later, with the growth of the Internet following the 1990s, Netizens rely on this informational

---

17 Stewart Baker, *USTR Wins the Crypto War*, Wash. Post (6 Nov. 2015), http://www.washingtonpost.com/news/volokh-conspiracy/wp/2015/11/06/ustr-wins-the-crypto-war/ (accessed 6 July 2016).

18 *See generally* David Kahn, *The Code-Breakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet* (Scribner 1967).

19 Jeffrey L. Vagle, *Furtive Encryption: Power, Trust, and the Constitutional Cost of Collective Surveillance*, 90 Ind. L.J. 101, 106–107 (2015).

20 Bert-Jaap Koops, *The Crypto Controversy: A Key Conflict in the Information Society* (Kluwer Law International 1999).

system for education, business, entertainment, and much more. Concerns over information security have therefore moved to the forefront.

Of vital importance to an information security system is 'cryptography' – an art that consists of creating secret writing by way of codes or ciphers[21] so that only intended recipients can read the message.[22] The process of transforming 'plaintext' into unreadable ciphertext is known as 'encryption'.[23] Decryption is the reverse process of returning ciphertext to its original form.[24] Mathematical algorithms are used in these transformational processes.[25]

Generally, encryption can be divided into symmetric and asymmetric systems. The former, also known as private-key, employs the same key to both encode and decode information.[26] Symmetric encryption has an inherent problem: because the key to encrypt the messages must be sent to the intended recipient, there is a risk that the key could be intercepted.[27] Thus, there is a chicken-and-egg problem: parties must exchange a key to communicate securely, but such exchanges take place through an insecure channel, which compromises the security before the encryption has even occurred.[28] It is particularly problematic when the list of the involved parties is large.[29] Such a drawback led to the creation of the asymmetric system, which employs two mathematically related keys: a public and a private key.[30] The public key is published or otherwise made available, and the sender uses it to encode messages and send the ciphertext to the recipient via an insecure channel[31]; the recipient then uses the private key to decrypt the information.[32]

---

21 *See* A. Michael Froomkin, *The Metaphor Is the Key: The Clipper Chip, and the Constitution*, 143 U. Pa. L. Rev. 709, 713 (1995) [hereinafter Froomkin, '*Metaphor*']; J. Terrence Stender, *Too Many Secret: Challenges to the Control of Strong Crypto and the National Security Perspective*, 30 Case W. Res. J. Int'l L. 287, 293 (1998).

22 John F. Dooley, *A Brief History and Cryptographic Algorithms* 4 (Springer 2013). The TPP Annex 8-B defines 'cryptography' as 'the principles, means or methods for the transformation of data in order to hide its information content,' prevent its undetected modification or prevent its unauthorized use; and it limited to the transformation of information using one or more secret parameters (e.g. crypto variables) or associated key management'. TPP Agreement, above n. 1, at Annex 8-B, para. 2.

23 Stender, above n. 21, at 293–294. For the definition of 'encryption' under the TPP, *see* above n. 10.

24 Koops, above n. 20, at 35.

25 Andres Rueda, *The Implications of Strong Encryption Technology on Money Laundering*, 12 Alb. L.J. Sci. & Tech. 1, 17–18 (2001).

26 Deborah Russell & G. T. Gangemi, Sr., *Encryption*, in *Building in Big Brother* 19 (Lance J. Hoffman eds, Springer 1995).

27 *See* RSA Laboratories, *Answers to Frequently Asked Questions About Today's Cryptography*, in *Building in Big Brother*, above n. 26, at 34.

28 Nathan Saper, *International Cryptograph Regulation and the Global Information Economy*, 11 Nw. J. Tech. & Intell. Prop. 673, 675 (2013).

29 National Research Council, *Cryptography's Role in Securing the Information Society* 53 (National Academy Press 1996) [hereinafter '*Cryptography's Role in Securing the Information Society*'].

30 This model was first introduced by Diffie and Hellman in 1976. Whitfield Diffie & Martin E. Hellman, *New Directions in Cryptography*, IT 22 (6) IEEE Trans. Inf. T. 644 (1976).

31 Greg Vetter, *Patenting Cryptographic Technology*, 84 Chi.-Kent. L. Rev. 757, 762 (2010).

32 *Ibid*.

The strength of an encryption system depends upon three factors: key management, algorithms, and key length.[33] Arguably, the latter two factors are less troublesome. Often, algorithms employed have been extensively tested to ensure mathematical security and the keys used are sufficiently long enough to resist brute-force attacks.[34] With good key generation, 'encryption keys are in most cases impossible to guess – trying to guess a single key could occupy a super-computer for millions of years'.[35] By contrast, the first factor that touches on the responsibility of users is problematic.[36] Thus, key management has become the most crucial task in the employment of encryption technologies for both the private and the public sector.[37] One way to manage the key is the idea of 'key escrow'.[38] By splitting an encryption key into several parts and distributing these parts to escrow agents or trusted third parties, these agents can, if necessary, help recovery and decoding.[39] These key management mechanisms, as argued below, have a bearing on regulatory intervention, and thus, trade barriers concerns.

2.2 Why does encryption matter?

Encryption contributes to personal, commercial, and political life by safeguarding the integrity, authenticity, and confidentiality of information.[40] To illustrate, this section considers the bright and the dark side of encryption by placing it in the context of privacy, commercial transactions, law enforcement, and national security.

2.2[a] *Information Security for Individuals and Businesses: A Civilian Perspective*

Every individual relies on encryption to secure online communications.[41] This is manifested by the robust development of encryption technologies in the private sector over the past decades. While, as detailed below, encryption had long been dominated by the military, the declining cost of computing technologies after the

---

33 Aaron Perkins, *Encryption Use: Law and Anarchy on the Digital Frontier*, 41 Hous. L. Rev. 1625, 1628 (2005).
34 Koops, above n. 20, at 42.
35 Orin S. Kerr, *The Fourth Amendment in Cyberspace: Can Encryption Create a 'Reasonable Expectation of Privacy'*, 33 Conn. L. Rev. 503 (2001).
36 Perkins, above n. 33.
37 *See* Saper, above n. 28, at 676.
38 For a background, *see* e.g. *Cryptography's Role in Securing the Information Society*, above n. 29, at 167–215.
39 D. Forest Wolfe, *The Government's Right to Read: Maintaining State Access to Digital Data in the Age of Impenetrable Encryption*, 49 Emory L.J 711, 717 (2000).
40 Lawrence Lessig, *Code 2.0*, 353 (Basic Books 2006).
41 Saper, above n. 28, at 677.

late 1960s and early 1970s sparked a surge of academic and commercial interest in this field.[42] In parallel with the rise of the networked communications, software vendors began to include encryption functionality in programs.[43] Microsoft, for instance, provided its BitLocker Driver Encryption utility free with the Windows Operating system since Vista Ultimate.[44] More recently, Apple introduced new encryption into its iPhone operating system, making cracking problematic.[45] Cryptography has also remained a top concern for the wireless sector.[46] For instance, the European Telecommunication Standards Institution (ETSI) included encryption algorithms called A5 in the Global System for Mobile Communications (GSM) to encode all communications between cellular phones and base stations.[47]

Besides firms in the high-tech sector, as noted above and elsewhere,[48] various emerging financial instruments and services in this increasingly globalized and electronically interconnected setting have placed banks and financial institutions far ahead of earlier users in private sectors when it comes to the application of encryption.[49] Data flow within banking system – such as the transmission of credit card numbers over the Internet or personal data used for the Automated Teller Machine (ATM) – should be enciphered to avoid an unrecoverable loss.[50] A digital signature underpinned by public-key cryptography helps to achieve the goal of 'nonrepudiation' by authenticating the identity of the parties and the content of the transactions.[51] The use of encryption has been extended to an array of civil applications, such as professional services, computer-based health care systems, petroleum industry, manufacturing, and entertainment industry.[52]

---

42 Whitfield Diffie & Susan Landau, *Privacy on the Line: The Politics of Wiretapping and Encryption* 315 (MIT Press 2007).

43 Joris V. J. Van Hoboken & Ira S. Rubinstein, *Privacy and Security in the Cloud: Some Realism About Technical Solutions to Transnational Surveillance in the Post-Snowden Era*, 66 Me. L. Rev. 487, 500 (2014).

44 *See* Paul Rubens, *Buyer's Guide to Full Disk Encryption* (9 May 2012), http://www.esecurityplanet.com/mobile-security/buyers-guide-to-full-disk-encryption.html (accessed 18 July 2016).

45 Danny Yadron, Spencer Ackerman & Sam Thielman, *Inside the FBI's Encryption Battle with Apple*, Guardian, http://www.theguardian.com/technology/2016/feb/17/inside-the-fbis-encryption-battle-with-apple (accessed 19 July 2016). Ironically though, with the third party's help, the FBI was nevertheless able to access the encrypted data. *See* e.g. CBS News, *FBI May Have Found Way to Unlock San Bernardino Shooter's iPhone* (21 Mar. 2016), http://www.cbsnews.com/news/fbi-may-have-found-way-to-unlock-san-bernardino-shooters-iphone/ (accessed 19 July 2016).

46 Koops, above n. 20, at 49.

47 It is reported however that the NSA can easily defeat A5/1 to intercept calls and texts. *See* e.g. Eli Biham & Orr Dunkelman, *Cryptanalysis of the A5/1 GSM Stream Cipher*, in *Progress in Cryptology–Indocrypt 2000* (Bimal Roy & Eiji Okamoto eds, Springer 2000).

48 Encryption technologies can also be applied to emails, facsimile, and Digital Versatile Disks (DVD), just to name a few. Froomkin, *Metaphor*, above n. 21, at 719–731.

49 It is reported that banking and financial firms are, after national governments, the second largest consumers of encryption technologies. *See* Anne C. Leer, *It's a Wired World: The New Networked Economy* 115 (Scandinavian University Press 1996).

50 Koops, above n. 20, at 52.

51 *Cryptography's Role in Securing the Information Society*, above n. 29, at 358.

52 *Ibid*., at 463–466; Froomkin, *Metaphor*, above n. 21, at 724; Koops, above n. 20, at 56.

2.2[b] *A Special Need of Governments: The Dark Side of Cryptography*

Governments, too, rely on a secure information system to carry out their functions. But governments also have other responsibilities beyond those of the private sector, including those related to public safety.[53] In law enforcement and national security, the importance of information security has long been recognized.

While cryptography secures personal privacy and commercial transactions, it can also be employed to provide a new scope for evil by offering terrorists groups and organized criminals a cost-effective way to engage in illegal activities.[54] Since the mid-1990s, for instance, the FBI has warned of such threats by identifying cases in which cryptography was applied to thwart criminal investigations.[55] Additionally, in the Tokyo subway sarin attack of 1995, Japanese authorities were unable to read encrypted computer files until they found the key on the diskette.[56] A more recent example is the Islamic States-led Paris attacks, which allegedly involved the use of encryption.[57]

Chief among concerns over encryption, however, is its military and diplomatic implications. Although cryptography has a centuries-long history of serving military purposes, it did not reach its prime until the beginning of the twentieth century, when wireless telephony was employed in World War I.[58] While radio enabled the transmission of military messages over long distances, it was more vulnerable to interception than other traditional channels previously employed. Since then, efforts have been made to develop mechanical devices to encode and decode messages.[59] Rapid developments of cryptography took place on both sides of the Atlantic as information itself became a major target of military and intelligence operations during World War II.[60] Notable examples of encryption applied to military purposes include Nazi Germany's Enigma,[61] Alan Turing's bombe,[62]

---

53 *Ibid*., at 46.

54 Stewart A. Baker & Paul R. Hurst, *The Limits of Trust: Cryptography, Governments, and Electronic Commerce* 5–6 (Kluwer Law International 1998); Thinh Nguyen, *Cryptography, Export Controls, and the First Amendment in Bernstein v. United States Department of State*, 10 Harv. J.L. & Tech. 667 (1997).

55 *Cryptography's Role in Securing the Information Society*, above n. 29, at 93.

56 Koops, above n. 20, at 65.

57 Rukmino Callimachi et al., *A View of ISIS's Evolution in New Details of Paris Attacks*, N.Y. Times (19 Mar. 2016), http://www.nytimes.com/2016/03/20/world/europe/a-view-of-isiss-evolution-in-new-details-of-paris-attacks.html?_r=0 (accessed 19 July 2016) (reporting that the fact that none of the attackers' electronic communications have been found prompted the authorities to believe that encryption technologies were used. What kind of encryption was used remained unclear, however).

58 Diffie & Landau, above n. 42, at 5.

59 All countries involved in the armed conflicts learned from the end of World War I that a faster and more effective way of secured communications is paramount from a national security perspective. Dooley, above n. 22, at 63.

60 *See* Koops, above n. 20, at 30.

61 For a detailed recount of Enigma, *see generally* Dooley, above n. 22, at 65.

62 *Ibid*., at 70–71.

and the US Navy's decisive victory in the Battle of the Midway.[63] During the Cold War, encryption was also applied to collect information about the military activities of the Soviet Union and Cuba.[64] Such war-time experience led many industrial countries to consider encryption as a 'dual-use' technology that – much like bombs and missiles – should be subject to restrictions long after the post-Cold War era.[65] This is the aspect of the crypto wars that implicates international economic order, as elaborated below.

3 INTERNATIONAL ECONOMIC LAW-MAKING IN THE SHADOW OF CRYPTO CONFLICTS

3.1 Born classified: encryption and war-time legacy

The war-time experience underscores encryption's dual-use character – that is, technologies characterized by both civilian and military values.[66] Therefore, many industrialized countries have subjected encryption to export control since the Cold War, albeit in different ways.[67] Americans were pioneers in tightening encryption controls.[68] Broadly, the US encryption policy has since then been guided by three major concerns. The first concern is to delay the worldwide spread of strong cryptographic capacities.[69] The second is to allow the country's high-tech firms to compete in foreign markets while maintaining regulatory control over the commercial development of cryptography at home.[70] The third is the capacity of terrorists and criminals to threaten national security.[71]

Shortly after the conclusion of World War II, the US reshaped its defense structure by passing the National Security Act of 1947.[72] This Act established the Department of Defense (DOD) to replace the War Departments of the Army, Air Force, and Navy, and to govern, via the NSA, the 'continued operation of an effective unified organization for the conduct of signals

---

63 Kahn, above n. 18, at 561–573.
64 Diffie & Landau, above n. 42, at 103.
65 Stender, above n. 21, at 328.
66 Sumner Benson, *The Security Perspective on Export Control Policy in the 1990s*, in *Export Controls in Transition: Perspectives, Problems, and Prospects* 9 (Gary K. Bertsch & Steven Elliott-Gower eds, Duke University Press 1992).
67 *See* Innokenty Pyetranker, *An Umbrella in Hurricane: Cyber Technology and the December 2013 Amendment to the Wassenaar Arrangement*, 13 Nw. J. Tech. & Intell. Prop. 153, 159–162 (2015); *Cryptography's Role in Securing the Information Society*, above n. 29, at 113.
68 Saper, above n. 28, at 677. *See also* below n. 89 and accompanying text.
69 *Cryptography's Role in Securing the Information Society*, above n. 29, at 114.
70 *Ibid*.
71 Tricia E. Black, *Taking Account of the World As It Will Be: The Shifting Course of the U.S Encryption Policy*, 53 Fed. Comm. L. J. 289, 297 (2001).
72 The National Security Act of 1947 (codified as amended at 50 U.S.C. § 401 et seq.).

intelligence activities'.[73] Since then, the NSA has long been dominant in US encryption policy by engaging in, among others, intelligence/counter-intelligence activities and identification of cryptographic items subject to export control under the International Traffic in Arms Regulations (ITAR) and the Export Administration Regulations (EAR),[74] implemented by the Department of State's Directorate of Defense Trade Controls (DDTC) and, more importantly, the Commerce Department's Bureau of Industry and Security (BIS), respectively.[75] An exporter seeking to sell encryption products falling within the lists designated by these agencies was subject to the review process, in which the NSA played a crucial role.[76] During the Cold War, these controls served as a geo-political strategy for the US to deter its adversaries, especially those from the Soviet bloc.[77] Other Western allies soon followed suit by establishing the Coordinating Committee for the Control of Multinational Trade, known as 'COCOM,' to block the transfer of arms, nuclear-related technologies, and dual-use items – including cryptography – to 'rogue states'.[78] It was not until the late 1980s that COCOM began to relax export controls on certain mass-market cryptographic software, although some members, especially the US, maintained rigorous regulations.[79]

Besides export controls, the US's National Bureau of Standards (later known as the National Institute of Standards and Technology, the NIST), with the involvement of the NSA, developed the Data Encryption Standard (DES) as a Federal Information Processing Standard to secure unclassified communications.[80] Somewhat paradoxically, while the government recommended DES as a secure system for use by the private sector, the NSA required IBM – the firm that

---

73 Robert N. Davis, *Striking the Balance: National Security vs. Civil Liberties*, 29 Brook. J. Int'l L. 175, 180–181 (2003).

74 The Export Administration Act (EAA) is the legislative basis for the EAR, which governs the dual-use items. *See Overview of US Export Control System*, http://www.state.gov/strategictrade/overview/ (accessed 2 Mar. 2016); Ian F. Fergusson & Paul K. Kerr, *The U.S Export Control System and the President's Reform Initiative*, CRS Report R41916, Congressional Research Service, 2–5 (13 Jan. 2014), http://www.fas.org/sgp/crs/natsec/R41916.pdf (accessed 4 July 2016); Dennis J. Burnett, *Ch. 13: United States of America*, in *Export Control Law and Regulations Handbook: A Practical Guide to Military and Dual-Use Goods Trade Restrictions and Compliance*, 352 (Yann Aubin & Arnaud Idiart eds, Kluwer International 2011).

75 Based on the Arms Export Control Act of 1947, the ITAR defines and specifies the US Munitions List. Fergusson & Kerr, *ibid.*, at 5–10.

76 Charles L. Evan, *U.S Export Control of Encryption Software: Efforts to Protect National Security Threaten the U.S Software Industry's Ability to Compete in Foreign Markets*, 19 N.C. J. Int'l L. & Com. Reg. 469, 479 (1994).

77 *Ibid.*, at 474, 477–478.

78 COCOM comprised of seventeen countries, including then the North Atlantic Treaty Organization (NATO) countries except Ireland, Australia, and Japan. *See generally* Burnett, above n. 74, at 11–30.

79 Koops, above n. 20, at 98.

80 *Cryptography's Role in Securing the Information Society*, above n. 29, at 417–418.

designed the algorithm called LUCIFER – to twist the structure by reducing the key length.[81] Although this seemed not to undercut the effectiveness of the DES – which has gained market acceptance for some thirty years,[82] such intervention reflected the US's concerns over the spread of strong cryptography.[83] The role of the intelligence agency in the standardization process for civilian use indicated the sensitive nature of cryptography in the post-war era. The Cold War experience, as illustrated below, implicated the way in which major trading powers crafted encryption policy, and thus, the relevant provisions of the TPP.

3.2 Crypto wars in the post-cold war era

With the collapse of the Soviet bloc, COCOM was replaced in 1996 by the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies (Wassenaar Arrangement).[84] The Wassenaar Arrangement was weakened by several political and economic factors. First, the lack of a common enemy made cooperation problematic among the Wassenaar members.[85] Second, unlike its predecessor, the Wassenaar Arrangement has no veto system; nor does it require notification prior to shipment. Thus, this Arrangement is implemented 'at the discretion of member governments pursuant to their own national policies'.[86] As American hegemony has eroded in the post-Cold War era, its Western allies begun to resist the COCOM-type order dominated by the US.[87] The need for the emerging high-tech industry to tap overseas markets further complicated the matter. This was particularly true in the case of dual-use items. Because military concerns could no longer justify rigid export control over dual-use items, Wassenaar members thus relaxed the rules by enabling the export of mass-market encryption products.[88]

---

81 Froomkin, *Metaphor*, above n. 21, at 889 (noting that 'as a result of its shorter key, DES is not considered sufficiently secure to protect classified data,' and yet, it was nevertheless certified by the NIST as suitable for commercial use). *See also* Lance J. Hoffman et al., *Cryptography Policy*, 37 (9) Commun. ACM 109, 110 (1994); John A. Fraser, *The Use of Encrypted, Coded and Secret Communications Is an 'Ancient Liberty' Protected by the United States Constitution*, 2 Va. J.L. & Tech. 2, 63 (1997). Cf. *Cryptography's Role in Securing the Information Society*, above n. 29, at 315–316 (arguing that 'DES is "good enough" for most information security applications').

82 Diffie & Landau, above n. 42, at 29.

83 *See Cryptography's Role in Securing the Information Society*, above n. 29, at 314.

84 The Wassenaar Arrangement, *About US*, http://www.wassenaar.org/about-us/ (accessed 27 July 2016).

85 Karim K. Shedhadeh, *The Wassenaar Arrangement and Encryption Exports: An Ineffective Export Control Regime that Compromises United States' Economic Interests*, 15 Am. U. Int'l L. Rev. 271, 298–299 (1999).

86 Christopher F. Corr. *The Wall Still Stands! Complying with Export Controls on Technology Transfers in the Post-Cold War, Post-9/11 Era*, 25 Hous. J. Int'l L. 441, 454 (2003).

87 Shedhadeh, above n. 85, at 298.

88 Koops, above n. 20, at 98.

Despite these changes, certain members like France, Russia, and the US, were more stringent than others.[89] Of particular interest to our discussion is the US's post-Cold War encryption policy. For years, the US executive branch had been struggling with its hard line approach towards encryption. Its dilemma reflected above-mentioned concerns. One recurring claim in favour of strict export control of encryption is national security: worldwide spread of strong encryption increases the costs for law enforcement and intelligence/counter-intelligence activities.[90] Such a claim was, however, undercut given the sea change in geo-politics in the post-Cold War era and the dynamic development of computing technologies. As stronger cryptography has become more accessible, the US's traditional approach has eroded its high-tech firms' competitiveness *vis-à-vis* their European counterparts in the global market.[91] Worse, losing the leadership in this field can be risky in both economic and national security terms since the US government agencies may not be able to break foreign-built encryption products should they fill the vacuum.[92] Also, while the US did not restrict the domestic purchase or use of strong encryption items by its citizens and permanent residents to protect against intrusions from hackers, illegal government investigations, and espionage by foreigners, its export control nevertheless affected the way in which academia and business community use and disseminate the encryption technology, thereby turning on constitutional debates under the First, Fourth, and Fifth Amendments, and had been challenged before the court on several occasions.[93]

To balance these competing interests, Congress has since the 1990s proposed several bills, seeking to move encryption policy from political and military spheres to a more commercial arena.[94] A major step was taken while President

---

89 For instance, while the Wassenaar members in 1998 agreed to place encryption items at 64-bit level on the mass-market products, the US only allowed the export of the encryption software up to the 56-bit length. Shedhadeh, above n. 85, at 299. For a detailed survey of encryption control, *see* e.g. Wayne Madsen et al., *Cryptography and Liberty: An International Survey of Encryption Policy*, 16 J. Marshall J. Computer & Info. L. 475 (1998).

90 Van Hoboken & Rubinstein, above n. 43, at 501 (noting that both the NSA and the FBI, facing the high-tech industry's lobby in the Congress and the Commerce Department, were against the dissemination of encryption products).

91 Shedhadeh, above n. 85, at 280–283.

92 *Cryptography's Role in Securing the Information Society*, above n. 29, at 156 ('Foreign vendors, by assumption, will be more responsive to their own national governments than to the U.S. government. To the extent that foreign governments pursue objectives involving cryptography that are different from those of the United States, U.S. interests may be adversely affected').

93 *See* e.g. *Karn v. Department of State*, 925 F. Supp. 1 (D.D.C. 1996); *Bernstein v. Department of State*, 974 F. Supp. 1288 (N.D. California 1997).

94 There are several proposed bills on encryption policies: the Encryption Communications Privacy Act of 1996 (ECPA), the Security and Freedom Through Encryption Act (SAFE), the Promotion of Commerce On-Line in the Digital Era Act (Pro-CODE), a revised version of the ECPA bill, and Secure Public Networks Act. For a history, *see* e.g. Stewart A. Baker & Michael D. Hintze, *Government*

Clinton took office.[95] The Clinton Administration sought to relax the review process, while proposing the 'Clipper Chip' endorsed by the NSA and the NIST.[96] The Clipper Chip employed 'key escrow' that works as follows: A master key was incorporated into the chipset at the time of fabrication in the US.[97] As compared to the DES standard, the Clipper Chip was equipped by the NSA with the Skipjack, an 80-bit algorithm that was much stronger and included – as an essential part of the Escrowed Encryption Standard (EES) – a specification adopted by the NIST for all secure communications equipment sold to government agencies.[98] The Skipjack was designed to protect against attempts to access its information.[99] Each chip-unique key was split into two pieces to be deposited with escrow agents located within the Departments of Commerce and Treasury, which would, upon the presentation of court orders, release the key to relevant authorities.[100] Clipper Chip program was modified as 'Clipper II', and later, 'Clipper III'.[101]

While the Clipper Chip providing US firms greater room to boost exports of their encryption products,[102] it was subject to harsh criticism. Among civil liberty organizations, such criticism turned on, again, constitutional debates.[103] For the high-tech industry, the Clipper Chip would not only impose additional costs, but frustrate their foreign customers, who were sceptical about products with a back door controlled by the US.[104] For instance, the Computer and Business Equipment Manufacturers Association, which represented various computer giants like Apple and IBM, remarked that 'foreign customers will not choose an encryption product that allows access by U.S. law enforcement agencies when other

---

Regulation of Encryption: Domestic and International Developments, http://encryption_policies.tripod.com/us/baker_060100_regulation.htm (accessed 21 July 2016).

95 Clinton's encryption policy reflected much of Vice President Gore's 1996 statement that the US government aimed to promote electronic commerce and robust Internet while protecting public safety and national security. The White House, Office of The Vice President, *Statement of the Vice President* (1 Oct. 1996).

96 For a background, *see Cryptography's Role in Securing the Information Society*, above n. 29, at 167–177.

97 *Ibid*., at 171.

98 Approval of Federal Information Processing Standards Publications 185, Escrowed Encryption Standard (EES), 59 Fed. Reg. 5997, 5997–5998 (9 Feb. 1994).

99 *Cryptography's Role in Securing the Information Society*, above n. 29, at 172.

100 *Ibid*.; A. Michael Froomkin, *It Came from Planet Clipper: The Battle over Cryptographic Key 'Escrow'*, U. Chi. L. Forum 15, 27 (1996).

101 For historical development of the Clipper Chip, *see* American Civil Liberties Union, *Big Brother in the Wires: Wiretapping in the Digital Age*, https://www.aclu.org/big-brother-wires-wiretapping-digital-age (accessed: 28 July 2016).

102 Froomkin, *Metaphor*, above n. 21, at 788.

103 Baker & Hurst, above n. 54, at 16.

104 *Ibid*. ('Business interests attacked the proposal as inflexible and expensive'); Van Hoboken & Rubinstein, above n. 43, at 501.

encryption products are readily available'.[105] Beyond the private sector, some agencies like the Department of Energy and the US Agency for International Development, were also against this proposal.[106]

Amid such noises, the Clinton Administration in 1996 sought to promote this idea via the Organization for Economic Cooperation and Development (OECD).[107] Major OECD members were split, however. While the UK[108] and France[109] supported the US in introducing the mandatory key recovery scheme, the Dutch, German, Japanese, and Scandinavian delegations all opposed this initiative.[110] Such opposition reflected the US allies' interest in tapping into the booming computer sector, and their distrust towards the role of US intelligence agencies in the high-tech industry.[111]

Diverging interests led the OECD to publish its 'Guidelines on Cryptography Policy' in March 1997, which rejected the mandatory key escrow scheme and government access requirement.[112] Instead, the OECD Encryption Guidelines stated explicitly that 'the development and provision of cryptographic methods should be determined by the market in an open and competitive environment'.[113] Immediately after the adoption of the OECD Encryption Guidelines, the European Commission dealt a major blow to the Clinton Administration via a publication entitled 'Toward a European Framework for

---

105 National Institute of Standards and Technology, *Hearing Before the Computer Security and Privacy Advisory Board* (27 May 1993) (quoting Vandana Pednekar-Magal & Peter Shields, *The State and Telecom Surveillance Policy: The Clipper Chip Initiative*, 8 Comm. L. & Pol'y 429, 444–445 (2003).

106 Susan Landau, *Under the Radar: NSA's Efforts to Secure Private-Sector Telecommunications Infrastructure*, J. Nat'l Sec. L. & Pol'y 411, 423 (2014).

107 The NSA, the Federal Bureau of Investigation (FBI), and the Department of Justice took the lead to lobby the OECD members to introduce the key escrow system. Pednekar-Magal & Shields, above n. 105, at 448.

108 The UK was the strongest supporter while the US promoted the mandatory key escrow scheme in the OECD. In 1999, the UK abandoned such attempt. Electronic Privacy Information Center, *Cryptography and Liberty 1999: An International Survey of Encryption Policy* 99 (EPIC 1999).

109 Traditionally, the French government adopted, according to the NSA, 'the most comprehensive cryptographic control' in Europe. Seeing cryptographic items as 'war materials', it was not until the mid-1990s that the French policymakers began to relax its control by introducing the Clipper Chip-type scheme. Madsen et al., above n. 89, at 496–497; Baker & Hurst, above n. 54, at 130–144.

110 Pednekar-Magal & Shields, above n. 105, at 449–450.

111 Germany was more liberal on the use and export of encryption. In drafting the OECD Encryption Guidelines, Germany's policymakers showed little interests in the US proposal for two major reasons. For one, Germany's high-tech firms often took advantage of the US's vigorous controls. For another, Germany was concerned about the risk that US-made computer hardware and software could be tampered by the NSA. *See* Shedhadeh, above n. 85, at 309.

112 Organization for Economic Cooperation and Development, *Guidelines for Cryptography Policy*, http://www.oecd.org/sti/ieconomy/guidelinesforcryptographypolicy.htm#background (accessed 27 July 2016) [hereinafter 'OECD Encryption Guidelines'].

113 *Ibid*.

Digital Signature and Encryption'.[114] In it, the European Commission rejected the concept of key escrow in light of its negative implications for privacy and electronic commerce. The fear that communications could be monitored with the help of key escrow, the European Commission argued, would lead individuals and companies to remain in the off-line world.[115]

A more decisive factor for Europe in rejecting the US proposal was, perhaps, the invisible hands of the US intelligence agencies in the standardization process. By the late 1990s, the 'ECHELON' became known to the public. As a joint effort among five Anglo-American countries – the US, the UK, Canada, Australia, and New Zealand – to intercept communications around the globe,[116] ECHELON raised the alarm for US allies across the Atlantic. Moreover, while its purpose was more national security oriented, this initiative was believed – and later confirmed – to involve industrial espionage.[117] For Europe, a response to such an intrusion was to relax the control over, thereby pressing Americans to curb their controls.[118] Beyond the OECD, the US also attempted to sell the idea of key escrow elsewhere in Asia, Africa, and Latin America, although these efforts were of limited scale.[119] Resistance from home and abroad pressed the US government to back down from the mandatory key recovery initiative; near the end of the Clinton Administration, many of these restrictions were further relaxed.[120]

3.3 A sense of déjà vu: emergence of crypto war 2.0 in the twenty-first century

The shifts to relax exports of encryption items resulted in a truce to the Crypto War in the late 1990s. Encryption controversy is, however, resurfacing given recent developments in, among others, India, Russia, Vietnam and, more crucially for our purpose, China. The return of enhanced restrictions over cryptography, we submit, is a major driver underlying the Encryption Clause.

In India, the Mumbai bombing of 2008 marked a major sea change since the nation has gradually moved away from its relatively more liberal approach towards encryption control.[121] The terrorist attacks led the Indian government to increase

---

114 Communication of the European Commission: Toward a European Framework for Digital Signatures and Encryption, COM (97) 503 final.

115 *Ibid*.

116 *See generally* Lawrence D. Sloan, *Echelon and the Legal Restraints on Signals Intelligence: A Need for Reevaluation*, 50 Duke L.J 1467 (2001).

117 Diffie & Landau, above n. 42, at 255.

118 *Ibid*., at 256.

119 Madsen et al., above n. 89, at 525–526.

120 Perkins, above n. 33, at 1640; Aimee Boram Yang, *China in Global Trade: Proposed Data Protection Law and Encryption Standard Dispute*, 4 *I/S* 897, 915 (2008–2009).

121 Madsen et al., above n. 89, at 500–501.

its capacity to lawfully intercept communications. In addition to entering a high-profile dispute with Research in Motion (RIM), a firm known for its BlackBerry, over keys to certain encrypted data,[122] the technical obstacles created by advanced cryptography have resulted in more stringent public control by India over the use of encryption products or systems of up to 40-bit length.[123] Despite objections from the high-tech industry at home and abroad, it is reported that India has been considering the possibility of a Clipper Chip-type scheme to ensure law enforcement agency access since 2011.[124] Worse, in 2012 India rolled out a new initiative called 'Preferential Market Access' (PMA). In a way, the PMA resembles China's MLPS, as detailed below, in that this policy aims to impose domestic preferences in procuring certain high-tech products – including encryption items – by both the public and the private sector.[125] The potential negative implications led to strong opposition by the US and others.[126]

Similarly, there have been regulatory initiatives in Vietnam and Russia towards a rigorous encryption scheme. In 2013, Vietnam issued the Draft Law on Information Security, proposing to treat 'civic' cryptography as a 'State secret' and subject its use to governmental oversight.[127] Additionally, despite the demise of the Soviet Union, Russia has maintained strict control over cryptography.[128] It restricts imports of products containing encryption, with the exception of its certified GOST algorithms,[129] which, together with other measures, raised concerns during its accession to the WTO.[130] The legacy of such practices can be found in certain former Soviet Union members like Kazakhstan and Kyrgyzstan –

---

122 *See* e.g. R. Jai Krishna, *India Sees Resolution to Blackberry Dispute*, Wall St. J. (8 Aug. 2012), http://www.wsj.com/articles/SB10000872396390443404004577576614174157698 (accessed 27 July 2016).

123 *See* Peter Swire & Kenesa Ahmad, *Encryption and Globalization*, 13 Colum. Sci. & Tech. L. Rev. 416, 442–443 (2012).

124 *Ibid*., at 444.

125 For a background, *see* Robert Hoffman, *Testimony at Subcommittee on Commerce, Manufacturing, and Trade, Committee on Energy and Commerce*, U.S. House of Representatives (27 June 2013), http://docs.house.gov/meetings/IF/IF17/20130627/101056/HHRG-113-IF17-Wstate-HoffmanR-20130627.pdf (accessed 27 July 2016); Takaaki Sashida, *Why Do We Need Encryption Rules in the TPP?*, Semiconductor Industry Association 6–7 (Sept. 2013).

126 *See* e.g. The Energy and Commerce Committee Press Release, *India to Reconsider Unfair Protectionist Policy*, https://energycommerce.house.gov/news-center/press-releases/india-reconsider-unfair-protectionist-policy (accessed 27 July 2016).

127 Some argued that the rule would violate Vietnam's WTO Accession Protocol. *See* e.g. Semiconductor Industry Association, *Comments Submitted Re: Draft 2.22 Law on Information Security, Issued by National Assembly, Socialist Republic of Vietnam* (10 July 2013), http://www.semiconductors.org/clientuploads/directory/DocumentSIA/International Trade and IP/SIA Comments on Draft Vietnam Encryption Regulations- FINAL.pdf (accessed 27 July 2016).

128 In Apr. 1995, President Yeltsin issued a Decree on 'Measures to Observe the Law in Development, Production, Sale and Use of Encryption Information.' The Decree banned the development, production, sale, and use of unlicensed encryption devices. Baker & Hurst, above n. 54, at 210.

129 Swire & Ahmad, above n. 123, at 449.

130 *See* above n. 13 and its accompanying text.

whose encryption policies were, at times, placed on the agenda of WTO trade negotiators.[131]

The rise of China as a major player in encryption policies, however, is perhaps most conspicuous. Like its former Communist counterparts, China has been conservative towards encryption since the Cold War.[132] In 1999, while China was negotiating WTO accession terms, its State Council institutionalized an encryption regime by issuing the Administration of Commercial Encryption Regulation (Encryption Regulation), thereby creating what is now known as the 'Office of Security Commercial Code Administration' (OSCCA).[133] According to the Encryption Regulation, almost every activity regarding commercial encryption items is subject to regulatory approval.[134] Thus, the sale of high-tech products with Chinese-made cryptography is restricted, in addition to those using foreign encryption technology.[135]

Such a catch-all approach gained new momentum after China envisaged itself as an emerging global technology leader in its Tenth Five-Year Plan (2002–2005).[136] Under the banner of 'indigenous innovation,' a policy goal set forth by the National Mid-Term and Long-Term Science and Technology Development Plan (2006–2020), China attempted to reduce its reliance upon Western technology by focusing on certain strategic industries.[137] Naturally, cybersecurity – a realm that has economic, political, and geo-political implications – has been at the forefront of the regulatory agenda. Many initiatives are reminiscent of this strategic plan.

---

131 *See* above n. 14 and its accompanying text; Trade Policy Review Body, *Trade Policy Review Report by Kyrgyz Republic* (1 Oct. 2013).

132 A firm wishing to import or export encryption products had been subject to licensing procedure under the auspices of the Ministry of Foreign Trade (now renamed as the Ministry of Commerce) or the foreign bureau of relevant provinces. Madsen et al., above n. 89, at 490–491; Baker & Hurst, above n. 54, at 106.

133 For a background, *see* e.g. Anne S.Y. Cheung, *The Business of Governance: China's Legislation on Content Regulation in Cyberspace*, 38 N.Y.U. J. Int'l L. & Pol. 1 (2005–2006).

134 Shang yong mi ma guan li tiao li [Administration of Commercial Encryption Regulations (promulgated by the St. Council, 7 Oct. 1999) [hereinafter '*Encryption Regulations*'].

135 While the SEMB in 2000 issued a memorandum, announcing that such restrictions would apply to 'only hardware and software for which encryption and decoding operations are core functions', and thus 'products in which encryption is only built-in (such as mobile phones and browser software) are exempted', the scope of application remains, in practice, far from clear. Baker & McKenzie, *China Legal Developments Bulletin* 11–12 (Apr.–June 2009) http://www.bakermckenzie.com/files/Uploads/Documents/Supporting%20Your%20Business/Recommended%20Reading/nl_china_legaldevelopmentsbulletin_aprjun09.pdf (accessed 27 July 2016).

136 Guo min jin gji he she hui fa zhan di shi ge wunian jihua (2001–2005) [The Tenth Five-Year Plan for the Development of National Economy and Society] (promulgated by People's Cong. Fourth Session, 15 Mar. 2001) (PRC).

137 Guo jia zhong chang qi ke ji fa zhan gui hua (2006–2020) [The National Mid-Term and Long-Term Science and Technology Development Plan (2006–2020)] (promulgated by the St. Council, 9 Feb. 2006).

Citing security flaws in the Wi-Fi, for instance, China in 2003 issued a wireless network standard equipped with its home-grown encryption technologies, called WAPI.[138] Despite its incompatibility with Wi-Fi, a standard used almost everywhere else, China mandated that all wireless devices must conform to WAPI before they can be placed on its market.[139] Possible trade barriers to sales of Wi-Fi-enabled products raised outcry among the high-tech sector and the trade community.[140]

For foreign companies, concerns are two-fold. First, because encryption technologies used in WAPI were owned by a handful of local Chinese firms, the implementation of this technical regulation would be tantamount to a sort of partnership between Western firms and their Chinese competitors in the manufacturing process.[141] Such cooperation would burden foreign firms in two ways. First, co-production would entail sharing information, some of which may not have been available without the WAPI.[142] Second, WAPI can impose extra transaction costs on foreign firms: in addition to the expenses of manufacturing two types of wireless devices, one used in China, the other throughout the rest of the world, they must bear the costs of authentication and royalties for WAPI-related technologies.[143] Second, and crucially, WAPI is somewhat reminiscent of the Clipper Chip-type encryption control during the post-Cold War era.[144] While China's policymakers in 2004 agreed to 'indefinitely postpone' WAPI after a high-level political dialogue with its American counterparts,[145] it has been criticized for being 'unwilling to approve

---

138 In 2001, researchers found that the Wired Equivalent Privacy (WEP) used in the Wi-Fi can be easily intercepted by an unauthorized user. Shortly after such findings, the creator of the Wi-Fi, the Institute of Electrical and Electronics Engineers (IEEE) began to fix the flaws via its IEEE 802.11 Task Group on Security. The result was the Wi-Fi Protected Access (WPA), a new encryption scheme later incorporated into the 802.11-series standard, now known as IEEE 802.11-i. *See* Nikita Borisov et al., *Intercepting Mobile Computing: The Insecurity of 802.11*, the Seventh Annual International Conference on Mobile Computing and Networking (Rome: Italy 2001), http://www.isaac.cs.berkeley.edu/isaac/mobicom.pdf (accessed 27 July 2016). *See also* above n. 15 and accompanying text.

139 Guo jia zhi liang jian du jian yan jian yi zong ju, guo jia bian zhun hua guan li wei yuan hui guan yu wu xian ju yu wang qiang zhi xing guo jia biao zhun shi shi de gong gao [Administration for Quality Supervision, Inspection, and Quarantine (AQSIQ) and Standardization Administration of China (SAC)'s Notification regarding Implementation of National Mandatory Standard for WLAN] (promulgated by AQSIQ and SAC) (26 Nov. 2003).

140 For a background, *see generally* Brian J. DeLacey et al., *Government Intervention in Standardization: the Case of WAPI* (Sept. 2006), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=930930 (accessed 27 July 2016).

141 *See* Yang, above n. 120, at 919.

142 *Ibid*.

143 *See* Christopher S. Gibson, *Globalization and the Technology Standards Game: Balancing Concerns of Protectionism and Intellectual Property in International Standards*, 22 Berkeley Tech. L. J. 1403, 1404, 1448–1149 (2007).

144 Saper, above n. 28, at 684.

145 DeLacey et al., above n. 140, at 12–13.

any Internet-enabled mobile handsets or similar hand-held wireless devices unless the devices were WAPI-enabled'.[146]

Beyond WAPI, the MLPS marks a new milestone in China's tightened control over encryption products. Launched in 2007 by the Ministry of Public Security and the Ministry of Industry and Information Technology (MIIT), the MLPS lays down a set of regulations governing cybersecurity for 'critical infrastructure'.[147] Specifically, it divides the information system into five levels, depending upon the extent to which a flaw in the system could threaten China's social order, public interest, and national security.[148] Each level has its own corresponding specifications for encryption; systems graded at level three and above are, moreover, required to use only those products developed by domestic firms, which must disclose source codes and encryption keys.[149] While the MLPS is purportedly only applied to critical infrastructure, its scope is, in fact, rather broad. Thus, much of the public and private sector has implemented relevant requirements.[150] Because the MLPS rules out the purchase of foreign products, it has received criticism from the EU, Japan, and the US, among others. While the MLPS has become a new battleground in the TBT Committee, it remains unclear whether a revised policy will ever see the light of day in the WTO.[151]

China's encryption control is somewhat reminiscent of what the US did during the Cold War and Post-Cold War eras. Indeed, China's intervention is multi-purpose and may not necessarily share an identical regulatory rationale with the US: for instance, the WAPI or MLPS scheme can serve to censor contents, which is unconstitutional in the US. One thing is for sure, however: neither China nor the US would accept the loss of control of cryptography – a 'key' that has economic and geo-political implications, as revealed by history. Backed by its formidable market power and rapid advances in technology, China has attempted to impose its home-grown ciphers on foreign enterprises through unilateral measures. Shaped by historical legacy and national security concerns, similar initiatives can be found in Vietnam, India, and former Soviet Union Member States. As the shadow of Crypto War 2.0 looms large, the US thus introduced the Encryption

---

146 The United States Trade Representative, *2014 Report on Technical Barriers to Trade* 57–58 [hereinafter '*2014 USTR TBT Report*'].

147 Dieter Ernst, *Indigenous Innovation and Globalization: The Challenge for China's Standardization Strategy* 33–34 (East-West Center 2011).

148 *2014 USTR TBT Report*, above n. 146, at 59.

149 *Ibid*., at 60.

150 The MLPS has, according to the USTR, been adopted by government agencies, firms in financial and telecommunications sectors, educational institutions, hospitals, and local companies operating power grids by way of request for proposals (RFPs).

151 *See* above n. 16 and accompanying text.

Clause to avoid protectionism in the cross-border transactions of encryption items. As argued below, however, challenges remain.

4 PROMISES AND DEMISES OF ENCRYPTION CLAUSE AND THE EVER-LASTING CRYPTO WAR

4.1 The promises of the encryption clause

The Encryption Clause marks a vantage point for the US in the Crypto War of the twenty-first century. By adding such clauses, which mirrors much of the OECD Encryption Guidelines, the US has moved encryption out of the shadows and into the normal world of business regulations. While the Clinton Administration failed to sell its Clipper Chip-type scheme through the OECD, the Guidelines nevertheless laid down key principles to avoid encryption policies that create unjustifiable barriers to trade and to the development of global networks.

As the Encryption Clause reveals, several overarching principles in the guidelines have been, explicitly or implicitly, included in the TPP. The guidelines underscore the market-driven approach to the development of cryptography and the importance of a variety of cryptographic methods based on users' choices.[152] The Guidelines read, in relevant part[153]:

> Although it is recognized that governments may influence product development by expressing, like any user, the need for a certain type of product, some believe governments should be careful not to drive markets in a particular fashion … Nevertheless, governments are also aware that if the requirements they impose on the use of cryptography are too burdensome, users of information and communications systems will not use cryptography and industry will not develop products that incorporate cryptographic techniques.

The Guidelines then called upon the OECD members to focus their standardization efforts on interoperability by bringing together systems using different cryptographic methods[154]:

> It is important for governments and industry to work together to provide the necessary architecture and standards so that information and communications systems can reach their full potential. A common description of an effective standard-setting process is one that is industry-led, voluntary, consensus-based and international.

Annex 8-B of the TPP follows the same line of thinking – user choice and market-driven – by prohibiting its participating countries from mandating a specific cipher or algorithm in the technical regulations or conformity assessment

---

152 OECD Encryption Guidelines, above n. 112.
153 *Ibid*.
154 *Ibid*.

for products used by or for non-governmental entities. Such a clause has implications for TPP and non-TPP parties. TPP parties must accept, by default, that manufacturers can choose encryption of their preference without concern about market access. Conceivably, measures like Vietnam's Draft Law on Information Security would be largely limited, if not abolished.

Besides anti-protectionism proxies like the necessity test, non-discriminatory principles, and international standards in TPP Chapter 8, Encryption Clause may also serve as an additional assurance to deter masked protectionism in the global trade of high-tech products. Legally, by structuring the Encryption Clause as a default rule, the TPP seemingly breaks the link between necessity and mandating the use of a particular cryptographic algorithm in the context of technical regulations. This is particularly true when taking into consideration paragraph 5 of Annex 8-B, which allows law enforcement authorities to require services providers to decode information subject to relevant legal proceedings.[155] The TPP parties may, put differently, require lawful access to encrypted information on a case-by-case basis; it would be unnecessary to link public interest and the encryption key through an overarching technical regulation. To this effect, the Encryption Clause can be seen as a TBT-Plus arrangement to reduce the digital protectionism.

Encryption Clause has broader implications beyond the TPP. For one, they signal to emerging economies with different preferences on encryption controls the 'best practice' in the context of global trade. Such best practices can serve as a template for future trade talks to reduce technical trade barriers to information products. In this light, the Encryption Clause may also serve to secure the liberalization that has already taken place under the aegis of the Information Technology Agreement (ITA). For another, presumably, by setting a high bar for encryption controls, the US could add disincentives to China's participation in the TPP, or at least pressure China to embrace the long-awaited revised policies.

4.2 The achilles tendon of the encryption clause

Despite the promises made by the TPP to eliminate the crypto war in the context of international trade, pitfalls remain. First, the Encryption Clause applies to products using cryptography and is designed for 'commercial applications'. Yet,

[155] TPP Agreement, above n. 1, at Annex 8-B, s. A, para. 5 ('For greater certainty, this section shall not be construed to prevent a Party's law enforcement authorities from requiring service suppliers using encryption they control to provide, pursuant to that Party's legal procedures, unencrypted communications'). Thus, in cases of, say, the recent encryption dispute between the FBI and Apple, the TPP parties would not be barred from requiring the key in accordance with the relevant proceedings.

because encryption has long been painted with dual-use characteristics, the term 'commercial application' can be contested. Reading this term may hinge upon, for instance, the end user of the relevant products or the length of the encryption key, thereby creating room for manoeuvring.

More crucially, national security remains a fatal blow to Encryption Clause as a useful mediator in Crypto War 2.0. In terms of 'national security,' our concerns extend beyond normative claims regarding whether and how countries may invoke security exceptions under TPP Article 29.2.[156] Rather, our concern is more an institutional one: Underlying security considerations may undercut the political will of non-TPP parties to accept the Encryption Clause as a template for future trade deals.

National security for the present purpose cuts both ways. In economic terms, for emerging economies, especially China and India, moving up the global value chain has been at the top of their regulatory agenda. Over the decades, these latecomers' economy has primarily consisted of manufactured goods that incorporate intellectual property rights (IPRs) owned by the West. Persistent disadvantage *vis-à-vis* Western counterparts may explain why, as seen in China's WAPI or India's PMA, home-grown cryptography – albeit in the name of cybersecurity, goes hand in hand with patented technologies controlled by local firms. Therefore, while the TPP attempts to protect proprietary encryption technologies by prohibiting members from requiring the transfer of algorithms or other secret parameters or entering into partnerships with local entities, in terms of technical regulations, it falls short of providing solutions to the deeply embedded problems in the ICT industry – that is, IPR issues in the manufacturing process.[157] Presumably, the Encryption Clause, alone, can barely stop the desire of these emerging economies to catch up with their global rivalries; cybersecurity is likely to serve as a pretext for protectionism.

In geo-political terms, national security concerns may render the already-tenuous Encryption Clause more fragile. That said, encryption was conceived and developed largely in response to World Wars. The geo-political rivalry between China and the US may give prominence to such a war-time legacy, thereby moving such dual-use technologies back into the shadow of power struggles. Since World War II, the US political leaders have perceived

---

[156] TPP Agreement, above n. 1, Art. 29.2 ('Nothing in this Agreement shall be construed to … preclude a Party from applying measures that it considers necessary for the fulfillment of its obligations with respect to the maintenance or restoration of international peace or security, or the protection of its own essential security interests').

[157] *See* Janice Muller, *Patent Misuse Through the Capture of Industry Standards*, 17 Berkeley Tech. L. J. 623 (2002); Mark Lemley, *Intellectual Property Rights and Standard-Setting Organizations*, 90 Cal. L. Rev. 1889 (2002).

technological superiority, as a matter of ideology, a military deterrence strategy.[158] Such an ideology has been translated into and entrenched by the decades-long 'military-industrial complex' and export controls over dual-use items.[159] While the US has relaxed its heavy-handed approach to encryption controls since the 1990s, today, it remains more problematic for Chinese enterprises and citizens than for those from other nations to access controlled technologies.[160] Such hostility has been accentuated by cyber espionage allegedly committed by Chinese intelligence and military units for business and political purposes in recent years.[161]

Ironically, though, while the US has been concerned about China tapping into its advanced technologies, Chinese leaders also seem cautious about the tie between America's intelligence agencies and high-tech industry, and thus, cryptography of US origin. The NSA was placed by President Reagan at the centre of cybersecurity, including encryption policy.[162] While Congress rejected a White House proposal to allow a role for the NSA in the development of cybersecurity for the private sector, the NSA made its way through the Computer Security Act of 1987. The Computer Security Act empowered the NIST to develop security standards for non-national security systems and to 'ensure the cost-effective security and privacy of sensitive information in Federal computer systems' by drawing upon, where appropriate, 'technical advice and assistance (including work product) of the National Security Agency'.[163] In 1989, these two agencies signed a memorandum to govern their cooperation, thereby creating a six-person technical working group to 'review and analyze issues … pertinent to protection of systems that process sensitive or other unclassified information'.[164] The Clipper Chip is an eminent example of such a joint effort between the NSA and NIST.

---

158 *See* e.g. Vannevar Bush, *Science: The Endless Frontier – A Report to the President* (United States Government Printing Office 1945), http://www.nsf.gov/od/lpa/nsf50/vbush1945.htm (accessed 27 July 2016)

159 Today, some argue further that the military-industrial complex seems to evolve into a 'military-cyber-intelligence mash-up'. Jim Wolf, *The Pentagon's New Cyber Warriors*, Reuter (5 Oct. 2010), http://www.reuters.com/article/us-usa-cyberwar-idUSTRE69433120101005 (accessed 27 July 2016).

160 *See generally* Bureau of Industry and Security, U.S. Department of Commerce, *Classification*, http://www.bis.doc.gov/index.php/policy-guidance/encryption/classification (accessed 27 July 2016)

161 P.W Singer & Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know* 57, 94–95 (Oxford University Press 2014) (arguing that China has persistently intruded into the networks of the public and private sectors in the US. Some intruders are political-oriented, while others seek to steal business secrets and IPRs).

162 In 1984, President Regan issued the 'National Security Decision Directive No. 145', giving the NSA broader authority over cybersecurity. White House, National Security Division Directive 145 – National Policy on Telecommunications and Automated Information Systems Security (17 Sept. 1984).

163 Computer Security Act of 1987, Pub. L. No. 100–235, s. 2(b) (1988).

164 *Memorandum of Understanding Between the Director of the National Institute of Standards and Technology and the Director of the National Security Agency Concerning the Implementation of Public Law 100–234* (23 Mar. 1989).

While the US government lost the battle of the key escrow in the late 1990s by moving towards a light-handed approach to encryption control, the NSA did not entirely fade away. According to internal documents leaked by Edward Snowden, a former NSA staffer, US intelligence units continue to insert 'back-doors' in all encryption after losing the crypto war in the 1990s.[165] Additionally, as a result of terrorist attacks over the last decade, the FBI's increasing interest in involvement in cybersecurity policies renders this already complex matter even more complicated.[166]

Such mutual distrust may operate to the contrary of the very aim of the Encryption Clause: that is, to bring peace to the crypto war. Worse, the fact that intelligence units work behind the scenes may undermine the credibility of international standardization bodies. For instance, the leaked documents indicate that the NSA has, through the NIST, affected the standards initiatives under the aegis of the International Organization for Standardization (ISO),[167] while contributing to the work through the Internet Engineering Task Force (IETF).[168] Such involvement may have a spillover effect by raising legitimacy concerns regarding these institutions, and their outputs as a relevant 'international standard' for the purpose of the TBT or the TPP. It remains to be seen how effectively the Encryption Clause could work towards a peaceful online environment in the long run.

5 FINAL REMARKS

While assessments of the impacts of trade agreements often take the legal text as the starting point and treat the disciplines as a given, one should not overlook the economic and geo-political contexts behind the text. This article goes beyond the text by unpacking the subtler, darker side of a trade deal. By using the Encryption Clause as a case study, we showcase how major powers leverage mega-PTA to shape the international economic order in this networked world.[169] The

---

[165] Nicole Perlroth et al., *N.S.A. Able to Foil Basic Safeguards of Privacy on Web*, N. Y. Times (5 Sept. 2013), http://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html?_r=0 (accessed 27 July 2016).

[166] *See* Landau, above n. 106, at 425–426.

[167] Nicole Perlroth, *Government Announces Steps to Restore Confidence on Encryption Standards*, N. Y. Times (10 Sept. 2013), http://www.nytimes.com/2013/09/11/us/court-upbraided-nsa-on-its-use-of-call-log-data.html (accessed 27 July 2016).

[168] Two NSA staffs, for instance, have signed up for the forthcoming IETF meeting for Apr. 2016. *See* IETF Meeting Registration System, Attendance List, IETF 95, http://www.ietf.org/registration/ietf95/attendance.py (accessed 27 July 2016); *see also* Landau, above n. 106, at 430.

[169] TPP Art. 14.17, for instance, may reduce the US's concerns over China's misappropriation of trade secret by protecting source code. For a critique of China's intervention in requiring access to source code, *see* United States International Trade Commission, *China: Intellectual Property Infringement, Indigenous Innovation Policies, and Frameworks for Measuring the Effects on the US Economy*, USITC Publication 4199, 4–11 (Nov. 2010).

Encryption Clause cannot be read in purely technical terms. Rather, one must contemplate a broader US-led trade campaign that is not just about traditional trade issues *per se*, but national security in the context of foreign policies. Secrecy is, as Michael Froomkin remarks, 'a form of power'.[170] Underlying the Encryption Clause is the power struggle between the US and its geo-political rivalries. In the absence of mutual trust, these new disciplines are only halfway to success. Crypto War 2.0 is not yet settled.

[170] Froomkin, *Metaphor*, above n. 21, at 712.