CHAPTER 5: ENCRYPTION SERVICES

5.1. Sector overview

Encryption supports digital trade as it protects the confidentiality and security of data, whether the data is in transit or storage. With encryption utilized in nearly all commonly used and globally traded ICT products and digital services, the adoption of policies that support encryption's role in protecting cross-border data flows supports digital trade, while discriminatory and restrictive policies could put digital trade and the large trade in ICT products at risk.

Encryption is a process to secure information from unauthorized access or use, mainly by changing information which can be read (plaintext) to make it so it cannot be read (cipher text)[89]. Over the last few decades, researchers and firms have gotten significantly better at using encryption to secure the privacy and integrity of data, which has been integrated into goods and services in order to improve security for consumers and businesses[90]. In particular, the development of public key cryptography, which allows users to communicate securely over an untrusted network, such as the Internet, has underpinned most modern ICT products and services. Whether consumers realize it or not, encryption is as ubiquitous as the many ICT devices they use in their daily lives. Even without a user's interaction, it is possible for devices to employ encryption when communicating to other devices to ensure that commands received from one device are authenticated before executing (US Department of Energy, 2011). Encryption is increasingly important as people and firms put more of their data online and engage with Internet-based services from throughout the world or use IT service providers from around the world.

Given this, encryption plays an important direct and indirect role in supporting digital trade. Encryption goods and services can be traded in-and-of themselves, such as through a software download. Encryption also plays a much broader role in supporting digital trade given it is embedded within many ICT goods and digital services. Encryption and other cryptographic tools can improve procedures for user authentication (preventing access from unauthorized actors) and guarantee the validity of instructions, as in the case of digital signatures[91]. As such, encryption allows consumers and firms to securely engage in a variety of online activities, such as access to services (e.g., logons, passwords, e-commerce applications) and privacy of communications (e.g., email, instant messaging, virtual private networks). Firms use encryption to protect the confidentiality of their research from competitors or hackers and to ensure the authenticity of their transactions with suppliers and customers. Essentially, strong encryption helps firms and consumers around the world securely communicate with the systems and individuals around the world, thereby facilitating the transactions that allow the global digital economy to grow (Jaikaran, 2016).

[89] Encryption is the act of scrambling the data, and decryption is the act of restoring the data to its original form. To encrypt or decrypt a key is needed. Cryptography can be described as a discipline, which embodies principles, means and methods for the transformation of data in order to hide its information content, prevent its undetected modification and/or prevent its unauthorized use. A cipher (or cypher) is an algorithm that transforms meaningful data into seemingly random data, and back again, when needed. Sweden's National Board of Trade, *The Cyber Effect The implications of IT security regulation on international trade* (Stockholm, June 2018), https://www.kommers.se/Documents/dokumentarkiv/publikationer/2018/The-Cyber-Effect.pdf.

[90] Daniel Castro and Alan McQuinn, *Unlocking Encryption: Information Security and the Rule of Law* (Washington, D.C: The Information Technology and Innovation Foundation, March, 2016), https://itif.org/publications/2016/03/14/unlocking-encryption-information-security-and-rule-law.

[91] Digital Europe and The Information Technology Industry Council, *ICT Recommendations for Regulatory Cooperation in the Transatlantic Trade and Investment Partnership* (Washington, D.C and Brussels, February 2, 2015), https://www.bitkom.org/sites/default/files/file/import/ICT-Industry-position-on-TTIP-Regulatory-Cooperation.pdf.s

Trade in and use of encryption goods and services still has significant room for growth, especially since the growing importance of cybersecurity and data privacy and security means that advances in encryption are at the forefront of competition in IT goods and services. Indicative of this growing sector is a 2016 survey by researchers from Harvard University which identified 865 hardware and software encryption products (a figure the researchers considered indicative and a lower-bound estimate) from 36 economies, with 56 percent of these products available for sale and 66 percent proprietary (while 34 percent are open source). Of the 546 non-U.S. encryption products the survey identified, 47 were for file encryption products, 68 email encryption products, 104 message encryption products, 35 voice encryption products, and 61 virtual private networking products (Schneier et al, 2016). Showing the room for growth, the Ponemon Institute's "2018 Global Data Security Study" survey of more than 3,200 IT and IT security officials from firms around the world found that while 95 percent have adopted cloud services, only 40 percent of them use encryption and key management services to securely store their data in the cloud.

5.2. **Profile of firm interviewed**

Virtru

Virtru's encryption services ensure that protection travels with the data—wherever the data is transferred and stored—as part of a user-friendly and client-side protected encryption service. Virtru's end-to-end encryption services are used by over 8,000 organizations and hundreds of thousands of users around the world, including for leading providers such as Gmail and Google Drive, Microsoft Outlook/Office 365, for a range of system-as-a-service cloud platforms, and for encryption key management. Virtru has been Google's Recommended Application Partner for encryption since 2016, enabling users to add layered protections to Gmail messages and attachments.

Virtru uses the trusted data format (TDF), an open source data protection standard. Regardless of whether the file is an email message, an Excel spreadsheet, or a photo, the files can be encrypted and "wrapped" into a TDF file. This file then communicates with Virtru-enabled key stores to maintain access privileges. For example, when the email recipient attempts to open the message and the attachments, the TDF "wrapper" communicates with the Virtru server and verifies whether the receiver is verified as eligible to access the data, after which (if approved), the user can decrypt, open, and read the files.

When combined with Virtru's key management and access control systems, TDF provides persistent protection and granular control for emails, files, and other data types. Virtru allows administrators to easily revoke a message so that a user on the other end of an email will have access to the email or attachments. Virtru also has audit tools that facilitate reporting on when and where email and files have been accessed or shared. Virtru uses this encryption technology to remove the complexity and obstacles that encryption services create for end users. For example, it allows users to search encrypted email and attachments as easily as they search Google or Microsoft email inboxes (which contrasts with other traditional encryption services). Virtru provides end-to-end encryption at the client-side so that emails and files are encrypted on the client end to protect data even before it gets sent. In contrast, many other cloud-based services only encrypt the data with a key shared between the user and the service provider, creating a vulnerability for the data because it can be exposed by the service provider.

5.3. **Role of data in firms' business models**

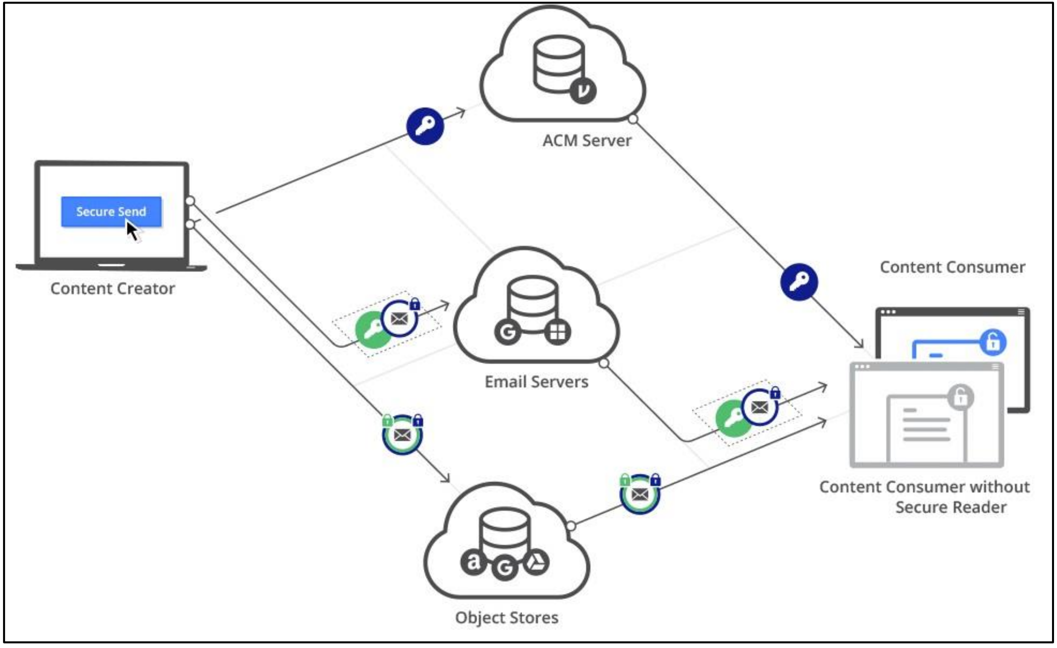
Data is central to Virtru's service and what its customers use it for. As it relates to the movement and storage of data, Virtru's encryption service means that data seamlessly crosses borders as part of each process (described below), unless artificial legal/regulatory barriers prevent or distort this. Data is critical to the movement of the underlying data that Virtru's encryption services protect, the accompanying service a customer might be using it as a part of (such as any number of common email and data storage providers), and the functioning of Virtru's service (given it involves parallel processes for the data to be protected, transferred, stored, and accessed).

Data privacy and protection are central to Virtru's business model. Clients use its services to protect certain categories of data to comply with legal requirements for firms to use technical measures to protect data, such as for personal, health, and financial data. However, just as important to Virtru, is that its service is able to be used as part of a broader IT service that allows users to continue to reap the benefits of being able to share data, but as part of a controlled and auditable process. Virtru's Zero Trust Architecture uses a split-knowledge approach to content protection. Content and encryption keys are stored separately, so that only authorized parties can access unencrypted content. Only recipients authorized by the content creator can access and decrypt protected content.

A key feature of Virtru's business model is ease-of-use. For example, Virtru allows authorized parties to receive and decrypt protected content without installing its software. When using Virtru to secure emails, all messages and attachments are encrypted with access control keys on the content creator's client via a browser extension, Microsoft Outlook plug-in, mobile app, or other Virtru-enabled client. Access control policies may also be applied at this time, such as authorizing a party's access, setting expiration for this access, and enhancing content protection via PDF watermarking or download disablement. Once encrypted, emails are sent via Transport Layer Security (TLS, and its predecessor, SSL, a point-to-point encryption used across the Internet to send secure email, protect financial transactions, and provide for secure web browsing) to the email server that will eventually deliver this content to authorized recipients. Cloud providers cannot access unencrypted content or decrypt content on their servers because they do not have access to the keys stored in the Virtru access control management (ACM) server.

To allow recipients to read emails without installing its software, Virtru utilizes an external object store, such as cloud storage services, to surface encrypted emails. The sending client that uses Virtru creates a copy of the encrypted email and any file attachments, re-encrypts them with a separate key, and sends the re-encrypted content to the designated object store. Virtru's services do not have access to the sender's or the recipient's email servers, ensuring that encrypted content stored in the external object store cannot be decrypted outside of a Virtru client. For each object, such as the individual email bodies and attachments, an individual Access Control Key is created and sent to Virtru's ACM. The content and key remain separate until a content consumer requests access to the encrypted email content. After authenticating, the content consumer receives access to both the Access Control Key (from the ACM) and the Split Knowledge Key (from the receiving email server). The Split Knowledge Key decrypts the Access Control Key, which decrypts the original email content. For file storage, many similar processes take place in email encryption. This process highlights the many and varied ways that data and data flows play in Virtru's business model.

Figure 10. Virtru's email encryption



Source: Virtru's website

5.4. How policies and regulations impact firms' business models

Commercial encryption services relate to several laws and regulations that affect—both positively and negatively—its role in digital trade. Many of these are detailed below, but in summary, include:

- The use of encryption as a tool to protect data privacy and ensure data security as required by an economy's laws;
- The need for licenses, registration, local encryption key storage, and source code disclosure as a condition of import, sale, and use for commercial encryption services and products;
- The need for firms to use a government-mandated encryption standard; and
- Legal and administrative requirements to provide vague and arbitrary decryption support or technical support, without a transparent, predictable, and independent legal framework to manage such requests.

Commercial encryption directly relates to a growing range of domestic and sectoral data privacy and protection laws around the world as a technical tool for firms to prove that they have taken reasonable steps to protect data, especially certain categories of data, such as personal, health, financial, and justice-related data (elaborated upon below). In many instances, encryption is not explicitly required (it is simply mentioned as an example of what should be used), while in other cases, encryption is explicitly required as a form of data protection, as is the case in a recent regulation from Denmark. Either way, effective encryption policies should satisfy local legal requirements for firms to take technical steps to protect data, while still allowing data to flow freely (i.e., to be transferred and stored anywhere).

Data-related laws and regulations that support the role and flow of data

Data-related laws and regulations can have a major effect on the data involved in the use of encryption services and the broader role that encryption plays in digital trade. The case with Virtru shows that economies can enact laws and regulations that mitigate data-related policy concerns through the use of technology, without affecting the flow of data (such as through local data storage requirements). Firms can use encryption services, such as with Virtru's, to comply with privacy, financial, data security, and other regulatory requirements that several economies have which require firms to use technical measures to protect data, especially certain categories of data considered sensitive. These encryption-related provisions (outlined below) focus on the firm using technological tools to ensure it protects certain categories of data, while still preserving its ability to transfer, share, and use data.

The United States

Health Data: Data encryption is a method to protect personal health information under the U.S. Health Insurance Portability and Accountability Act (HIPAA), which extends to all data that a covered entity creates, receives, maintains, or transmits in electronic form[92]. For example, HIPAA requires integrity controls (to ensure data is not improperly modified) and that organizations use a mechanism to encrypt electronic health information. For example, Omada Health uses Virtru's services to share sensitive data, including via email, whereas previously, it could not do this as its previous email and security arrangements were not secure enough. Furthermore, Virtru's service scans emails upon sending and matches them against specific rules to alert users that they may contain sensitive information and should therefore be encrypted. Similarly, Pitkin County in the United States and Massena Hospital both adopted Virtru's encryption services to ensure HIPAA compliance and better protect privacy and security.

Ultimately, this means that these organizations can send and share sensitive data with authorized third-parties, such as those involved in email, cloud storage, backup storage, mobile apps, tech support, and data analytics. Protecting healthcare data is critical as electronic health records can be worth even more to hackers than some financial data, such as credit card numbers, as the data (a person's insurance details, social security number, address etc.) can be used to create fake IDs to buy medical equipment or drugs (which can be resold) or used to file fraudulent insurance claims[93]. This healthcare data is often included in human resources data for foreign firms with U.S. operations. For example, Sony Pictures, which operates outside of the healthcare industry but still has human resources-related HIPAA requirements, has struggled to adequately secure healthcare data in the cloud. Following its 2014 email hack, Sony sent out a breach notification email admitting that info covered by HIPAA policy was among the leaked data[94].

Payments data: Encryption of cardholder data is an acceptable method of rendering data unreadable in order to meet the Payment Card Industry Data Security Standard (PCI DSS), which is a set of security controls that businesses are required to implement to protect credit card data. This is an industry-required standard (it is not required by U.S. law) managed by the Payment Card Industry (PCI) Security Standards Council. IT platforms need to be certified to manage this payments data, and while some popular cloud-based communications storage services have not been certified, when used in conjunction with Virtru's encryption services (which is certified), firms are able to use these popular platforms to manage cardholder data from the United States outside the economy.

The European Union (EU)

Privacy and Encryption – The EU's General Data Protection Regulation (GDPR) emphasizes data governance and accountability when firms manage personal data, requiring firms to assess the risk of data loss and data breach and requires them to consider technical—"state of the art"—measures to

[92] "Summary of the HIPAA Security Rule," U.S. Health and Human Services website, https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html

[93] Caroline Humer and Jim Finkle, "Your medical record is worth more to hackers than your credit card," *Reuters*, September 24, 2014, https://www.reuters.com/article/us-cybersecurity-hospitals-idUSKCN0HJ21I20140924

[94] Steve Ragan, "Sony Pictures admits HIPAA data might have been compromised during breach," *CSO Online,* December 15, 2014, https://www.csoonline.com/article/2859822/business-continuity/sony-pictures-admits-hipaa-data-might-have-been-compromised-during-breach.html

mitigate those risks, including encryption. Because encryption is a common security measure and cybersecurity risks are increasing, it is likely that regulators and courts in Europe will find that encryption is necessary to comply with GDPR. The European Union Agency for Information and Network Security (ENISA) recommendation for end-to-end encryption for email supports this likely outcome[95]. Indicative of this assessment, Denmark's data protection agency announced in July 2018 that firms must encrypt all emails transmitting sensitive personal data[96]. This means that firms can use encryption systems, such as Virtru's, to transfer Danish personal data overseas (subject to other regulations).

Virtru's encryption services satisfy encryption-related requirements in the GDPR as they provide a level of protection and a range of access control features, such as protecting emails from creation (not once it reaches the email server), while allowing users and administrators to decide who can access content (and for how long). Relevant to the GDPR's governance and accountability requirements, email and file forwarding services using Virtru's system can be audited, limited, or prevented altogether. For example, Return Path (a leading email marketing firm) uses Virtru's encryption services to protect confidential human resources information and sensitive client communications in the European Union. In the past, the firm used Pretty Good Privacy, but it was not user-friendly, whereas Virtru's application can be turned on/off at the click of a button, is integrated with existing email providers, works with existing single sign-on processes, and provides protection for files and from a broader range of cyber threats. Again, this allows firms that use Virtru's services to transfer and use personal data from the European Union overseas (subject to other regulations).

Furthermore, while GDPR does not include specific rules for key management, Virtru's end-to-end key management services relate to requirements for technical security measures relating to encryption keys. Virtru allows customers to store encryption keys on-premise or in any cloud platform in order to give them exclusive control over encrypted content. This is in line with ENISA recommendations that "it is preferable, from a privacy perspective" that service providers do not have access to keys.

Multilateral engagement on commercial encryption issues

While commercial encryption services have existed for some time, international engagement to deal with domestic and international issues are limited. As of today, the most comprehensive international effort to establish recommended encryption policies took place in the Organization for Economic Co-operation and Development (OECD) in 1997 with the non-binding "OECD Guidelines for Cryptography Policy." Even back then, OECD members recognized that "due to the inherently global nature of information and communications networks, implementation of incompatible [domestic] policies will not meet the needs of individuals, business and governments and may create obstacles to economic co-operation and development; and, therefore, [domestic] policies may require international co-ordination."

Modern trade agreements have started including provisions to protect the trade in, and role of, encryption goods and services. For example, the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) includes a number of provisions in the technical barriers to trade chapter, including ones that prohibit an economy from requiring a firm to transfer or to provide access to proprietary encryption technology and material, such as a private key or algorithm specification as a

[95] European Union Agency for Network and Information Security, "Privacy and Data Protection by Design" (Heraklion, Greece, January 12, 2015), https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design

[96] Murtha Cullina, "Denmark Implements Email Encryption Requirement, What Countries Will Follow?" *JDSupra*, July 25, 2018, https://www.jdsupra.com/legalnews/denmark-implements-email-encryption-41045/

condition of market entry, sale, distribution, import, or use[97]. Furthermore, it prohibits signatories from requiring a firm from having to setup a joint venture or use a particular cryptographic algorithm, while providing exceptions for government networks, law enforcement access (via a legal process), supervision of financial institutions or markets, and for domestic security issues. The draft United States–Mexico–Canada Agreement also prohibits import restrictions of commercial goods that contain cryptography[98]. The European Union also views securing rules to protect encryption as a key component of its digital trade strategy[99].

Data-related laws and regulations that limit the role and flow of data

There are a range of laws and regulations related to encryption services that potentially inhibit or stop the flow of data. These include: requirements that firms store encryption keys locally; requirements relating to government access to data (such as requests for decryption or technical assistance), even though this may not be technically feasible given encryption key access issues; and requirements relating to government approval for market entry, such as source code disclosure and the use of mandatory encryption standards.

For example:

- Local encryption key storage would mean that the firm or its customer would have to setup a local server to facilitate the authentication and encryption process. For customers using their service outside their home economy, this would mean that the data allowing the encryption key authentication and use would flow back-and-forth across a border.
- Data localization would mean that use of encryption services would be limited to within that economy's borders. The only cross-border data flows involved in using encryption services would happen for categories of data that do not need to be stored locally.
- If economies require the disclosure of a firm's source code as a condition of market entry, it would limit market access as it would dissuade some firms from entering given the potential adverse impact of source code misappropriation. Similarly, government requests for technical assistance or encryption keys pose a similar potential barrier to market entry and operations as facilitating such requests may pose broader risks to the security and reputations of a firm and its IT products.

These types of rules would potentially affect the flow of data for firms like Virtru that focus on commercial encryption services. It should be noted that Virtru did not report that it or its clients have run into these issues. However, a number of economies have considered or enacted these types of requirements, which would affect data involved in its type of service. For example, as part of its broader strategy to control data within its borders, one APEC economy is increasingly requiring encryption keys and data access, with non-complying firms potentially being fined or having limited market access[100].

[97] Annex 8-B. "Chapter 8: Technical Barriers to Trade," New Zealand Ministry of Foreign Affairs and Trade, https://www.mfat.govt.nz/assets/Trans-Pacific-Partnership/Text/8.-Technical-Barriers-to-Trade-Chapter.pdf

[98] United States Trade Representative, "United States-Mexico-Canada Trade Fact Sheet," United States Trade Representative Office website, https://ustr.gov/about-us/policy-offices/press-office/fact-sheets/2018/october/united-states%E2%80%93mexico%E2%80%93canada-trade-fa-0

[99] Marietje Schaake, *Working Document on Towards a digital trade strategy*, (Brussels, Committee on International Trade, European Parliament, June 7, 2017), https://marietjeschaake.eu/media/uploads/posts/1497947344-Working%20Document%20Marietje%20Schaake%20Towards%20a%20Digital%20Trade%20Strategy%20INTA.pdf

[100] Josiah Wilmoth, "Russia May Unban Telegram…if it Shares Encryption Keys with the FSB," CCN, August 28, 2018, https://finance.yahoo.com/news/russia-may-unban-telegram-shares-133955770.html; Amy MacKinnon,

Similarly, other APEC economies have required local data storage and government access to data, which in effect requires breaking encryption[101]. Another APEC economy has also passed recent legislation that would require companies to not use end-to-end encryption in commercial products so law enforcement could gain access to data. Such efforts that mandate data access may effectively weaken security and privacy[102].

Market Entry or Operating Requirements

Commercial encryption services can also be affected through a range of other legal, technical, and administrative requirements, especially when the laws and legal framework for rules are broad, vague, intrusive, and implemented without a legal avenue for appeal.

Licensing and registration requirements can be used to limit which firms can enter, how they can operate, and what they can develop and use in terms of encryption products and services[103]. For example, some economies require an import permit or license for a range of encryption products and have an extensive certification regime to manage the development, distribution, use, and sale of encryption products[104]. As part of recent reforms in one APEC economy, firms need to obtain a certificate to produce encryption products, while distributors can only distribute certified products[105].

Similarly, requirements that firms provide source code disclosure for information communication technology (ICT) products (which have encryption embedded) as part of vague and broad security certification reviews can be used as a tool to discriminate against foreign products across a number of major commercial sectors, such as banking, finance, health, and other sectors[106]. Likewise, mandatory encryption key disclosure as part of law enforcement or domestic security investigations, such as under the Investigatory Powers Act of one non-APEC economy, raise trade concerns given the potential for users to see this as an indirect weakening of an encryption product/service. Another example, mandatory

"How Russia is Strong-Arming Apple," Foreign Policy, January 31, 2019, https://foreignpolicy.com/2019/01/31/how-russia-is-strong-arming-apple-data-security-icloud/; Maria Kolomychenko, "Exclusive: Russia plans stiffer fines for tech firms that break rules – sources," Reuters, November 26, 2018, https://www.reuters.com/article/us-russia-technology-security-exclusive-idUSKCN1NV09P.

[101] Campbell Kwan, "New Thai laws allow government to access information without warrants: Report," ZDNet, March 1, 2019, https://www.zdnet.com/article/new-thai-laws-allow-government-to-access-information-without-warrants-report/; Jeff Paine, RE: Additional Submission with comments on Thailand's Cyber Security Bill (Singapore, Asia Internet Coalition letter to Thailand's Ministry of Digital Economy and Security, November 29, 2018), https://www.aicasia.org/wp-content/uploads/2018/12/Final-AIC-additional-comments-for-Thai-CS-BIll_291118.pdf; Aekarach Sattaburuth, "Cybersecurity bill passed," Bangkok Post, February 28, 2019, https://www.bangkokpost.com/news/general/1636694/cybersecurity-bill-passed.

[102] Jamie Tarabay, "Australian Government Passes Contentious Encryption Law," New York Times, December 6, 2018, https://www.nytimes.com/2018/12/06/world/australia/encryption-bill-nauru.html.

[103] Global Partners Digital, *World map of encryption laws and policies*, website, https://www.gp-digital.org/world-map-of-encryption/

[104] Covington, *China Revises Rules on Commercial Encryption Products*, Covington law firm website, October 15, 2017, https://www.cov.com/-/media/files/corporate/publications/2017/10/china_revises_rules_on_commercial_encryption_products.pdf

[105] De Brauw Blackstone Westbroek, *Trends – China moves away from strict encryption regulations for foreign companies*, De Brauw Blackstone Westbroek website, February 15, 2018, https://www.debrauw.com/newsletter/trends-china-moves-away-strict-encryption-regulations-foreign-companies/#

[106] Michael Martina, "Business groups petition China's premier on cyber rules," *Reuters,* August 11, 2016, https://www.reuters.com/article/us-cyber-china-business-idUSKCN10M1DN

encryption standards, also constitute a technical barrier to trade as it prevents a firm from using its own proprietary encryption standard and process, which allows easier integration for the firm's global operations and may be more secure. For example, one APEC economy has mandated the use of domestic encryption products in telecommunications infrastructure, such as for 4G[107].

Intellectual Property

Commercial encryption services can also be affected through intellectual property-related laws and regulations that mandate that firms provide access to or a copy of their underlying source code. This poses a significant risk to a firm's business model, as source code lies at the heart of the patented technology that encryption companies develop to secure goods and services. For example, one APEC economy is considering mandatory source code disclosure as part of a new law for electronic systems and transaction operations[108]. While the details of industry-standard encryption algorithms are generally available, the implementation of these algorithms as part of a software or hardware product to deliver commercial goods and services may be proprietary. Sharing source code with government agencies risks poses a number of issues, such as potential source code misappropriation. In exceptional cases, such as in government procurement, there may be legitimate reasons to require source code disclosure, but a blanket requirement for encryption key or source code disclosure as a condition of market access is significantly disproportionate and trade distorting.

Concerns about source code disclosure also arise when economies mandate broadly defined requirements that firms cooperate or provide technical support to regulatory, law enforcement, and domestic security agencies, such as for security reviews as part of licensing and certification and for law enforcement and domestic security investigations. Beyond the risks from source code disclosure, the integrity of a firm's encryption products may be undermined by mandating that firms build so-called "back doors" into their products to facilitate government access. This can raise concerns such as defining technical requirements based only on an economy's subjective view of what is reasonable and practical, without due regard for how encryption is developed or how it works.[109] A weakness or opening provided for one stakeholder inevitably weakens the overall level of protection as it provides an opening for others, such as hackers. There have been calls for and draft laws mandating such cooperation and back doors in several APEC economies. In contrast, both Germany and the Netherlands have publicly disavowed backdoors in encryption products.[110]

Encryption key management is another area where economies can enact trade-distorting measures, such as requiring a firm to store keys within an economy (a so-called "key escrow"). Key management includes dealing with the generation, exchange, storage, use, and replacement of keys. In economic terms, it could be argued that an encryption key represents the aggregated value of all the information

[107] Adam Segal, *China, Encryption Policy, and International Influence.* (Stanford, Hoover Institute, 2016), https://www.hoover.org/sites/default/files/research/docs/segal_webreadypdf_updatedfinal.pdf; Stephen Ezell, *The Middle Kingdom Galapagos Island Syndrome: The Cul-De-Sac of Chinese Technology Standards* (Washington, D.C: The Information Technology and Innovation Foundation, 2014),

[108] "Letter: comments on Government Regulation 82/2012 on Electronic Systems and Transaction Operations," multiple trade association letter, hosted on the Software Alliance website, March 1, 2018, https://www.bsa.org/~/media/Files/Policy/Data/03012018BSAJointSubmissionOnGR82Amendment.pdf

[109] Aaron Tan, "Apple challenges Australia's proposed decryption law," *Computer Weekly*, October 15, 2018, https://www.computerweekly.com/news/252450584/Apple-challenges-Australias-proposed-decryption-law

[110] Kim Zetter, "Encryption is Worldwide: Yet Another Reason Why A U.S. Ban Makes No Sense," *Wired*, February 11, 2016, https://www.wired.com/2016/02/encryption-is-worldwide-yet-another-reason-why-a-us-ban-makes-no-sense/; "Dutch government says no to 'encryption backdoors'," *BBC*, January 7, 2016, https://www.bbc.com/news/technology-35251429. https://www.bbc.com/news/technology-35251429

that is protected by it, for example, all bank transactions.[111]. For example, Apple moved encryption keys for iCloud account users into one economy in response to a new cybersecurity law.[112].

5.5. Conclusion

Encryption services play both a direct role (given their growing use) and indirect role (as a facilitator of communications and other services) in digital trade. By acting as a technical tool to protect data and data-driven services, encryption services provide a clear example as to how the confidentiality of data does not generally depend upon its location, but the technical and administrative tools used to store and secure it. Yet, encryption services' role in digital trade can be limited by policies which restrict the free flow of data it relies on (through data localization), customer choice of services (through licensing and other market entry restrictions), the intellectual property it can be protected by (such as source code disclosures), and key technological processes which ensure its integrity (such as encryption keys and government-mandated backdoors).

[111] Sweden's National Board of Trade, *The Cyber Effect The implications of IT security regulation on international trade* (Stockholm, June 2018), https://www.kommers.se/Documents/dokumentarkiv/publikationer/2018/The-Cyber-Effect.pdf

[112] Stephen Nellis and Cate Cadell, "Apple moves to store iCloud keys in China, raising human rights fears," *Reuters*, February 24, 2018, https://www.reuters.com/article/us-china-apple-icloud-insight/apple-moves-to-store-icloud-keys-in-china-raising-human-rights-fears-idUSKCN1G8060; Robert McMillan and Tripp Mickle, "Apple to Start Putting Sensitive Encryption Keys in China," *Wall Street Journal,* February 24, 2018, https://www.wsj.com/articles/apple-to-start-putting-sensitive-encryption-keys-in-china-1519497574