Cryptography: How India Regulates Encryption

Irfan Jalal Bhat [1] Dr. Raghav Mehra [2]
Dr. Amit Kumar Chaturvedi[3]

[1] Research. Scholar, Computer Application, Bhagwant Univeristy Ajmer (India)

[2]Associate Professor & Dean Student Welfare Bhagwant Institute of Technology, Muzaffarnagar (India)

[3] Assistant Professor MCA Departement Govt. Engineering College, Ajmer Rajasthan (India)

ABSTRACT:

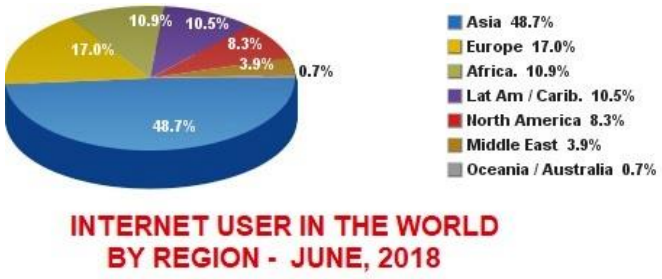
Mobile security, or more specifically mobile device security, has become increasingly important in mobile computing. Of particular concern is the security of personal and business information now stored on Smartphone. More and more users and businesses use smartphones to communicate, but also to plan and organize their users' work and also private life. In this paper we bring the survey of Smartphone user in india, also bring the concept of Encryption and Data Vulnerability in India. The crypto wars in India may have lessons to learn from the conflict between Silicon Valley and the United States government. Still, there are many unique considerations that Indian policymakers must keep in mind. In this paper we concluded that while studying a regulatory framework for encryption it is necessary that we identify the lens through which encryption is looked at i.e. whether encryption is considered as a means of information security or a threat to national security.

Keywords - Security, Encryption, Vulnerability, Cyberspace, symmetric keys.

I. INTRODUCTION

The concept of efficiency and optimization work that is accommodated in a single device, indirectly alter people's behavior toward smartphones from needs becoming dependency. The new 2018 Global Digital suite reports from We AreSocial and Hootsuitereveals that there are now more than 4 billion people around the world using the internet.Well over half of the world's population is now online, with the latest data showing that nearly a quarter of a billion new users came online for the first time in 2017. Africa has seen the fastest growth rates, with the number of internet users across the continent increasing by more than 20 percent year-on-year.Much of this year's growth in internet users has been driven by more affordable smartphones and mobile data plans. More than 200 million people got their first mobile device in 2017, and two-thirds of the world's 7.6 billion inhabitants now have a mobile phone. More than half of the handsets in use today are 'smart' devices too, so it's increasingly easy for people to enjoy a rich internet experience wherever they are.Social media use continues to grow rapidly too, and the number of people using the top platform in each country has increased by almost 1 million new users every day during the past 12 months. More than 3 billion people around the world now use social media each month, with 9 in 10 of those users accessing their chosen platforms via mobile devices.You'll find the key insights from this year's reports in our more detailed analysis below, but here are the essential headlines for digital in 2018:

- The number of internet users in 2018 is **4.021 billion**, up 7 percent year-on-year.
- The number of social media users in 2018 is **3.196 billion**, up 13 percent year-on-year
- The number of mobile phone users in 2018 is **5.135 billion**, up 4 percent year-on-year

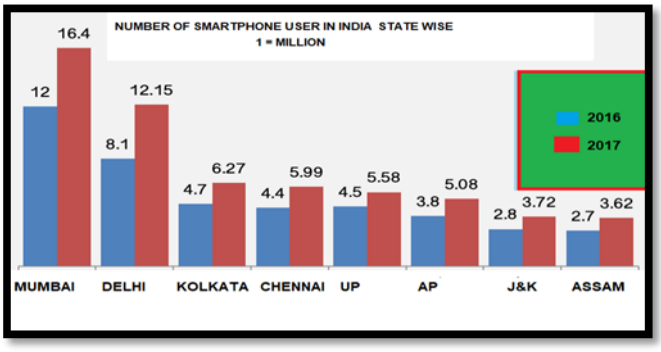


INTERNET USER IN THE WORLD
BY REGION - JUNE, 2018

The rate of smartphone adoption will continue to be robust, as their users register a double-digit growth. Almost 2.10 billion people or 28.7% of the world's population will own smartphones by the end of 2016. The increase in the number of smartphones users will also be faster than that of feature phones. Nearly 47.4% of mobile phone users will possess smartphones by the end of this year. By the end of 2017, smartphone users will outnumber feature phone users.

II. INTERNET USAGE IN INDIA - STATISTICS & FACT

The number of internet users in India is expected to reach 500 million by June 2018, said a report by the Internet and Mobile Association of India (IAMAI) and Kantar IMRB on Tuesday. The number of Internet users stood at 481 million in December 2017, an increase of 11.34% over December 2016 said the report titled, "Internet in india 2017".Urban India with an estimated population of 455 million already has 295 million using the internet. Rural India, with an estimated population of 918 million as per 2011 census, has only 186 million internet users leaving out potential 732 million users in rural india. "Given that total Urban Population is much lower than total rural population, the Urban-Rural Digital divide is actually more acute than what the penetration numbers portray. The future growth policies therefore must focus on bridging the digital divide that exists between urban and rural India today," the report added. Internet penetration in Urban India was 64.84% in December 2017 as compared to 60.6% last December. In comparison, rural Internet penetration has grown from 18% last December to 20.26% in December 2017. With over 460 million internet users, India is the second largest online market, ranked only behind China. By 2021, there will be about 635.8 million internet users in India.



III. ENCRYPTION AND DATA VULNERABILITY IN INDIA.

The crypto wars in India may have lessons to learn from the conflict between Silicon Valley and the United States government. Still, there are many unique considerations that Indian policymakers must keep in mind. India's domestic legal system, after all, suffers from a lack of privacy legislation, inadequate data protection rules, and a surveillance regime that is, for the most part, guided by colonial legislation. How the country regulates encryption will have implications on rights, commerce and national security. It will need to harmonise the regulatory landscape so that the multifarious interests of various stakeholders are balanced. There is no explicit Constitutional recognition of the right to privacy in India. Instead, it has emerged through a series of pronouncements by Indian courts to gain recognition as a penumbral right under other fundamental freedoms. This position, however, is tenuous at best. The government, through the Attorney General, has claimed that there is no right to privacy available to Indian citizens.[11] The Supreme Court of India, in 2015, convened a Constitution Bench to adjudicate upon the issue.[12] The apex court is expected to finally rule on the contours of the right within the next year. In the meantime, traditional privacy-based arguments against decryption of information by the government are not as readily applicable. This is further complicated by India's surveillance regime which lacks safeguards in the form of judicial review. Interception of communications in India is authorised by an executive order under Section 5(2) of the Telegraph Act, 1885 and Section 69B of the Information Technology Act, 2000 (hereinafter IT Act).[13] Orders of interception under Section 5(2) also follow improperly defined standards such as "on the occurrence of public emergency" or "expedient… in the interest of national security as preconditions.[14] Similarly, under Section 69B, the government can order collection of information from any computer resource to "enhance cyber security." Without the guidance of a privacy law, orders for surveillance are left to the subjective determination of a non-judicial authority. These broad powers of interception can also include access to encrypted information. The Data Protection Rules drafted under Section 87(2)(ob) of the IT Act classify passwords as "sensitive personal data or information".[15] Password, in turn, has been defined to include encryption and decryption key.[16] However, the rules also mandate that a body corporate that collects this sensitive data will share it with a government agency upon receiving a request in writing.[17] As a result, India's data protection laws have faced criticism both at home and overseas.[18] The European Union, for one, views Indian data protection regulation as being inadequate for European data. A recent survey by the Data Security Council of India (DSCI) estimates that this may have resulted in an opportunity loss of USD 2-2.5 billion.[19] Even technical standards that are available for data protection do not prescribe a high standard for encryption. Earlier, the licensing agreement between the Indian Department of Telecommunications and Internet Service Providers (ISPs) stipulated that no ISP would be permitted to use encryption standards higher than 40-bit symmetric keys.[20] Any use of higher encryption would involve obtaining express approval from the government and the submission of decryption keys. The license agreement also prohibited the use of bulk encryption by ISPs. Curiously, the Unified Licensing Agreement that replaced the erstwhile service-specific licensing agreements dropped the upper limit mandating 40-bit encryption. It, however, retained the prohibition on bulk encryption and specified that the use of encryption by the ISP's subscriber will be governed by a policy drafted under the Information Technology Act.[21] The absence of the 40-bit standard has removed an upper ceiling on what is permissible encryption, but the rule has not been supplanted by any provision that clarifies the issue. Taken together, the absence of a privacy law, excesses of surveillance powers, and the

inadequacy of data protection norms create inconsistent policies that are not conducive to investments and growth in technology. The Draft Policy was a reflection of these inconsistencies. Shortly after the release of the Draft Policy in 2015 the government issued a clarification that mass-market encryption products would be excluded from the ambit of the policy; that effectively excluded services like WhatsApp and standards like OpenSSL from the policy's effects. It is unclear whether the second iteration of the encryption policy will apply to mass-market encryption tools. It, however, should. A "good" encryption policy can have the effect of harmonising the regulatory landscape around information security, in turn triggering changes to decades-old laws. It is noteworthy that this time around, the Ministry of Electronics and Information Technology is seeking inputs from industry bodies and civil society while drafting the policy. This is an opportunity to avoid the same pitfalls that the Draft Policy suffered from. It is also a time to analyse and learn from other jurisdictions that have seen similar debates.

IV HOW INDIA REGULATES ENCRYPTION

Governments across the globe have been arguing for the need to regulate the use of encryption for law enforcement and national security purposes. Various means of regulation such as backdoors, weak encryption standards and key escrows have been widely employed which has left the information of online users vulnerable not only to uncontrolled access by governments but also to cyber-criminals. The Indian regulatory space has not been untouched by this practice and constitutes laws and policies to control encryption. The regulatory requirements in relation to the use of encryption are fragmented across legislations such as the Indian Telegraph Act, 1885 (Telegraph Act) and the Information Technology Act, 2000 (IT Act) and several sector-specific regulations. The regulatory framework is designed to either limit encryption or gain access to the means of decryption or decrypted information.

A. LIMITING ENCRYPTION

The IT Act does not prescribe the level or type of encryption to be used by online users. Under Section 84A, it grants the Government the authority to prescribe modes and methods of encryption. The Government has not issued any rules in exercise of these powers so far but had released a draft encryption policy on September 21, 2015. Under the draft policy, only those encryption algorithms and key sizes were permitted to be used as were to be notified by the Government. The draft policy was withdrawn due to widespread criticism of various requirements under the policy of which retention of unencrypted user information for 90 days and mandatory registration of all encryption products offered in the country were noteworthy. The Internet Service Providers License Agreement (ISP License), entered between the Department of Telecommunication (DoT) and an Internet Service Provider (ISP) to provide internet services (i.e. internet access and internet telephony services), permits the use of encryption up to 40 bit key length in the symmetric algorithms or its equivalent in others. The restriction applies not only to the ISPs but also to individuals, groups and organisations that use encryption. In the event an individual, group or organisation decides to deploy encryption that is higher than 40 bits, prior permission from the DoT must be obtained and the decryption key must be deposited with the DoT. There are, however no parameters laid down for use of the decryption key by the Government. Several issues arise in relation enforcement of these license conditions.

1. While this requirement is applicable to all individuals, groups and organisations using encryption it is difficult to enforce it as the ISP License only binds DoT and the ISP and cannot be enforced against third parties.
2. Further, a 40 bit symmetric key length is considered to be an extremely weak standard[22] and is inadequate for protection of data stored or communicated online. Various sector-specific regulations that are already in place in India prescribe encryption of more than 40 bits.
3. The Reserve Bank of India has issued guidelines for Internet banking[23] where it prescribes 128-bit as the minimum level of encryption and acknowledges that constant advances in computer hardware and cryptanalysis may induce use of larger key lengths. The Securities and Exchange Board of India also prescribes[24] a 64-bit/128-bit encryption for standard network security and use of secured socket layer security preferably with 128-bit encryption, for securities trading over a mobile phone or a wireless application platform. Further, under Rule 19 (2) of the Information Technology (Certifying Authorities) Rules, 2000 (CA Rules), the Government has prescribed security guidelines for management and implementation of information technology security of the certifying authorities. Under these guidelines, the Government has suggested the use of suitable security software or even encryption software to protect sensitive information and devices that are used to transmit or store sensitive information such as routers, switches, network devices and computers (also called information assets). The guidelines acknowledge the need to use internationally proven encryption techniques to encrypt stored passwords such as PKCS#1 RSA Encryption Standard (512, 1024, 2048 bit), PKCS#5 Password Based Encryption Standard or PKCS#7 Cryptographic Message Syntax Standard as mentioned under Rule 6 of the CA Rules. These encryption algorithms are very strong and secure as compared to a 40 bit encryption key standard.
4. The ISP License also contains a clause which provides that use of any hardware or software that may render the network security vulnerable would be considered a violation of the license conditions.[25]Network security may be compromised by using a weak security measure such as the 40 bit encryption or its equivalent prescribed by the DoT but the liability will be imputed to the ISP. As a result, an ISP which is merely complying with the license conditions by employing not more than a 40 bit encryption may be liable for what appears to be contradictory license conditions.
5. It is noteworthy that the restriction on the key size under the ISP License has not been imported to the Unified Service License Agreement (UL Agreement) that has been formulated by the DoT. The UL Agreement does not prescribe a specific level of encryption to be used for provision of services. Clause 37.5 of the UL Agreement however makes it clear that use of encryption will be governed by the provisions of the IT Act. As noted earlier, the Government has not specified any limit to level and type of encryption under the IT Act however it had released a draft encryption policy that has been suspended due to widespread criticism of its mandate.
6. The Telecom Licenses (ISP License, UL Agreement, and Unified Access Service License) prohibit the use of bulk encryption by the service providers but they continue to remain responsible for maintaining privacy of communication and preventing unauthorized interception.

B. GAINING ACCESS TO MEANS OF DECRYPTION OR DECRYPTED INFORMATION

Besides restrictions on the level of encryption, the ISP License and the UL Agreement make it mandatory for the service providers including ISPs to provide to the DoT all details of the technology that is employed for operations and furnish all documentary details like concerned literature, drawings, installation materials and tools and testing instruments relating to the system intended to be used for operations as and when required by the DoT.[26] While these license conditions do not expressly lay down that access to means of decryption must be given to the government the language is sufficiently broad to include gaining such access as well. Further, ISPs are required to take prior approval of the DoT for installation of any equipment or execution of any project in areas which are sensitive from security point of view. The ISPs are in fact subject to and further required to facilitate continuous monitoring by the DoT. These obligations ensure that the Government has complete access to and control over the infrastructure for providing internet services which includes any installation or equipment required for the purpose of encryption and decryption. The Government has also been granted the power to gain access to means of decryption or simply, decrypted information under Section 69 of the IT Act and the Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009.

1. A decryption order usually entails a direction to a decryption key holder to disclose a decryption key, allow access to or facilitate conversion of encrypted information and must contain reasons for such direction. In fact, Rule 8 of the Decryption Rules makes it mandatory for the authority to consider other alternatives to acquire the necessary information before issuing a decryption order.
2. The Secretary in the Ministry of Home Affairs or the Secretary in charge of the Home Department in a state or union territory is authorised to issue an order of decryption in the interest of sovereignty or integrity of India, defense of India, security of the state, friendly relations with foreign states or public order or preventing incitement to the commission of any cognizable offence relating to above or for investigation of any offence. It is useful to note that this provision was amended in 2009 to expand the grounds on which a direction for decryption can be passed. Post 2009, the Government can issue a decryption order for investigation of any offence. In the absence of any specific process laid down for collection of digital evidence do we follow the procedure under the criminal law or is it necessary that we draw a distinction between the investigation process in the digital and the physical environment and see if adequate safeguards exist to check the abuse of investigatory powers of the police herein.
3. The orders for decryption must be examined by a review committee constituted under Rule 419A of the Indian Telegraph Rules, 1951 to ensure compliance with the provisions under the IT Act. The review committee is required to convene atleast once in two months for this purpose. However, we have been informed in a response by the Department of Electronics and Information Technology to an RTI dated April 21, 2015 filed by our organisation that since the constitution of the review committee has met only once in January 2013.

V. CONCLUSION

While studying a regulatory framework for encryption it is necessary that we identify the lens through which encryption is looked at i.e. whether encryption is considered as a means of information security or a threat to national security. As noted earlier, the encryption mandates for banking systems and certifying authorities in India are contradictory to those under the telecom licenses and the Decryption Rules. Would it help to analyse whether the

prevailing scepticism of the Government is well founded against the need to have strong encryption? It would be useful to survey the statistics of cyber incidents where strong encryption was employed as well as look at instances that reflect on whether strong encryption has made it difficult for law enforcement agencies to prevent or resolve crimes. It would also help to record cyber incidents that have resulted from vulnerabilities such as backdoors or key escrows deliberately introduced by law. These statistics would certainly clear the air about the role of encryption in securing cyberspace and facilitate appropriate regulation. By study the different research paper here are the some solution are as

- The present Modi government must take cyber security of the country seriously considering the ever-increasing cyber security challenges in India.
- It is time now that India must be cyber prepared to protect its cyberspace.
- Draft of the National cyber security policy of India 2018 should be completed as soon as possible.
- There must be a dedicated cyber security law of India keeping in mind contemporary cyber security threats.
- Also cyber security disclosure norms in India must be formulated.
- The cyber security awareness in India must be further improved and spread so that various stakeholders can also effectively take part to the implementation of cyber security initiatives of Indian government.

VI. Acknowledgements

We feel grateful to the referees for their valuable suggestions that have helped immensely in preparing the revised manuscript.

REFERENCES

[1] http://www.digitalpolicy.org/going-dark-in-india-the-legal-and-security-dimensions-of-encryption/

[2] Wilfred Diffie and Susan Landau, “Privacy on the Line: The Politics of Wiretapping and Encryption,” MIT Press, (Cambridge, 2007), p. 13

[3] Kaveh Waddell, “The Long and Winding History of Encryption,” The Atlantic, January 13, 2016, http://www.theatlantic.com/technology/archive/2016/01/the-long-and-winding-history-of-encryption/423726/.

[4] Nicolas Lidzborski, “Staying at the Forefront of Email Security and Reliability: HTTPS-Only and 99.978% Availability,” Official Gmail Blog,March20,14, https://gmail.googleblog.com/2014/03/staying-at-forefront-of-email-security.html.

[5] WhatsApp Support Team, “End-to-End Encryption,” WhatsApp.com, accessed November10,2016, https://www.whatsapp.com/faq/en/general/28030015.

[6] Telegram, “MTProto Mobile Protocol,” Telegram.org, accessed November 10, 2016, https://core.telegram.org/mtproto.

[7] Apple Inc. “iOS Security Whitepaper,” Apple Inc., May 2016 accessed November 10, 2016, https://www.apple.com/business/docs/iOS_Security_Guide.pdf.

[8] US Law enforcement, in the 1970s called for a ban on hard drive encryption of Microsoft

[9] Berkman Center for Internet & Society at Harvard University, "Don't Panic: Making Progress on the "Going Dark" Debate," Berkman Center for Internet & Society at Harvard University, February 1, 2016, https://cyber.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf.

[10] Steven Levy, "Why Are We Fighting the Crypto Wars Again?," Backchannel, March 11, 2016, https://backchannel.com/why-are-we-fighting-the-crypto-wars-again-b5310a423295#.saxlftve3.

[11] Press Trust of India, "'Right to Privacy Not a Fundamental Right': Centre Tells Supreme Court,"NDTV,July3,2015, http://www.ndtv.com/india-news/right-to-privacy-not-a-fundamental-right-centre-tells-supreme-court-784294.

[12] Sidharth Pandey, "Is Privacy a Fundamental Right? Constitution Bench of Supreme Court to Decide,"NDTV,August11,2015, http://www.ndtv.com/india-news/is-privacy-a-fundamental-right-constitution-bench-of-supreme-court-to-decide-1206100.

[13] Information Technology Act, 2000, §69(B)

[14] Bedavyasa Mohanty, "Inside the Machine: Constitutionality of India's Surveillance Apparatus," IJLT Issue 12 (To be published)

[15] Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, Rule 3(i)

[16] Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, Rule 2(1)(h)

[17] Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, Rule 6(1)

[18] See, Bhairav Acharya, "Comments on the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011", Centre for Internet and Society, March 31, 2013, http://cis-india.org/internet-governance/blog/comments-on-the-it-reasonable-security-practices-and-procedures-and-sensitive-personal-data-or-information-rules-2011

[19] NASSCOM, "NASSCOM Update on EU Data ProtectionRegime,"ASSCOM http://www.nasscom.in/sites/default/files/policy_update/EU%20data%20Protection%20Regulation.pdf

[20] Department of Telecommunications, "Licence Agreement For Provision Of Internet Service (Including Internet Telephony) Amendments," Department of Telecommunications, Ministry of Communications, Government of India, accessed November 11, 2016, Clause 1.10.1, http://dot.gov.in/granted-issue-guidelines.

[21] Department of Telecommunications, "License Agreement For Unified License," Department of Telecommunications,

[22] Schneier, Bruce (1996). Applied Cryptography (Second ed.). John Wiley & Sons

[23] Working Group on Information Security, Electronic Banking, Technology Risk Management and Cyber Frauds- Implementation of recommendations, 2011

[24] Report on Internet Based Trading by the SEBI Committee on Internet based Trading and Services, 2000; It is useful to note that subsequently SEBI had acknowledged that the level of encryption would be governed by DoT policy in a SEBI circular no CIR/MRD/DP/25/2010 dated August 27, 2010 on Securities Trading using Wireless Technology

[25] Clause 34.25 of the ISP License

[26] Clauses 22 and 23 of Part IV of the ISP License

[27] Reserve Bank of India, Report and Recommendations of the Working Group on Information Security, Electronic Banking, Technology Risk Management and Cyber Frauds(2011) available at http://cab.org.in/IT%20Documents/WREB210111.pdf

[28] Securities and Exchange Board of India, Report of the Committee on Internet-Based Securities, Trading and Services(2000) available at http://111.93.33.222/RRCD/oDoc/29-nettrading_200059.pdf(Accessed September 3, 2016)

[29] Matt Tait, "An Approach to James Comey's Technical Challenge," Lawfare, April 27, 2016, https://www.lawfareblog.com/approach-james-comeys-technical-challenge.

[30] Ashley Deeks, "The International Legal Dynamics Of Encryption, "Hoover Institution, Series Paper no. 1609,accessedNovember10,2016, http://www.hoover.org/research/international-legal-dynamics-encryption.

[31] Human Rights Watch, "Russia: 'Big Brother' Law Harms Security, Rights," Human Rights Watch, July 12, 2016, https://www.hrw.org/news/2016/07/12/russia-big-brother-law-harms-security-rights.

[32] Monitoring and Reconciliation of International Telephone Traffic Regulations, 2010, Regulation 5(6), http://www.pta.gov.pk/media/monitoring_telephony_traffic_reg_070510.pdf.

[33] Kaveh Waddell, "Kazakhstan's New Encryption Law Could Be a Preview of U.S. Policy," The Atlantic,December8,2015, http://www.theatlantic.com/technology/archive/2015/12/kazakhstans-new-encryption-law-could-be-a-preview-of-us-policy/419250/.

[34] Digital Rights LAC, "The Dangerous Ambiguity of Communications Encryption Rules in Colombia" Digital Rights Latin America and the Caribbean, January30,2015, http://www.digitalrightslac.net/en/la-peligrosa-ambiguedad-de-las-normas-sobre-cifrado-de-comunicaciones-en-colombia/.

[35] Emily Rauhala, "China Passes Sweeping Anti-Terrorism Law With Tighter Grip on Data Flow," Washington Post, December 28, 2015, https://www.washingtonpost.com/world/china-passes-sweeping-anti-terrorism-law-with.-tighter-grip-on-data-flow/2015/12/28/4ac6fe06-d79b-4c4c-bda9-27f15fabf892_story.html?tid=a_inl

[36] Bruce Schneier, Kathleen Seidel, and Saranya Vijayakumar, "A Worldwide Survey of Encryption Products," Berkman Klein Centre for Internet and Society at Harvard University, February 11, 2016, https://cyber.harvard.edu/publications/2016/encryption_survey.

[37] Thorsten Benner and Mirko Hohmann, "The Encryption Debate We Need," Global Public Policy Institute, May 19, 2016, http://www.gppi.net/publications/global-internet-politics/article/the-encryption-debate-we-need/.

[38] Mark Hosenball and Dustin Volz, "Exclusive: White House Declines to Support Encryption Legislation – Sources," Reuters, April 7, 2016, http://www.reuters.com/article/us-apple-encryption-legislation-idUSKCN0X32M4.

[39] Trans-Pacific Partnership, Technical Barriers to Trade, Paragraph 5, Section A, Annexure 8-B, https://ustr.gov/sites/default/files/TPP-Final-Text-Technical-Barriers-to-Trade.pdf

[40] Trans-Pacific Partnership, Technical Barriers to Trade, Paragraph 3, Section A, Annexure 8-B, https://ustr.gov/sites/default/files/TPP-Final-Text-Technical-Barriers-to-Trade.pdf

[41] Jeremy Malcolm, "Has the TPP Ended the Crypto Wars? Hardly.," Electronic Frontier Foundation, November18,2015, https://www.eff.org/deeplinks/2015/11/has-tpp-ended-crypto-wars.

[42] A blockchain is a peer-to-peer shared digital ledger that maintains records of transactions. Every participant has an identical copy of the ledger.