

Thai Citizens and their roles in National Security of Thailand

Srirath Gohwong

¹ Faculty of Social Sciences, Kasetsart University, Thailand. Email: srirathg3@yahoo.com

ABSTRACT

The objective in this study was to investigate the state of art of Thai citizens and their roles in national security of Thailand. Documentary research was employed in this study. The findings revealed that Thai citizens played a big role as both supporters and objectors for national security of Thailand due to both external and internal changes. As supporters of Thai government's jurisdiction, good citizens must comply with IT-related laws that allowed Ministry of Digital Economy and Society (MDES) and related authorized agencies that enhanced the level of controlling on data via surface web sites. As objectors, they committed civil disobedience-oriented activities beyond Thai government's jurisdiction via the application of privacy-based non-governmental cryptocurrency (such as Monero) and web browsers for underground web sites (such as TOR and I2P) for hiding all data of their identities and money transfer. In addition, Thai citizens were also protected by net states as citizen-user in a form of business civil disobedience.

Keywords: Thai Citizens, National Security, Thailand

Article Received: 18 October 2020, Revised: 3 November 2020, Accepted: 24 December 2020

Significance of problem

National security has been one of the most favorite topics in Public Administration since 1900 or the first paradigm of this nice field of study according to Nicholas Henry's classification (Henry, 2013). It depends on two components of every modern state according to the Article 1 of The Convention on Rights and Duties of States (inter-American) on December 26, 1933 – government and citizens (Convention on Rights and Duties of States, 1933; White, 1926; Marini, 1971; Frederickson, 1989; Osborne and Gaebler, 1992; Peters, 2001; O'Leary, Van Slyke, Kim, 2010; Henry, 2013; Shafritz, Russel, Borick, 2017). However, the emerging of many advanced IT technologies (such as IoT, Deep Web and Dark Web, cryptography, Blockchain and Cryptocurrency, TOR (The Onion Browser), I2P, and 5G) and the emerging of net states, an amount of tech firms that provide many services like state, have directly attacked national security by allowing citizens to obey or disobey their governments (Gohwong, 2017, 2018a; 2018b; 2019a; 2019b; 2020; Laudon and Laudon, 2020; Wichowski, 2020).

For Thailand as an important nation-state in ASEAN community, it has faced this challenge on

its national security since the first day of Bitcoin on 3 January 2009. After that day, nineteen laws (such as Constitution of the Kingdom of Thailand 2017, National Security Council Act 2016, Ministry Enhancing Act (Book no.17) 2016 (Establishing the Ministry of Digital Economy and Society), Computer-related Crime Act (No.2) 2017, the Emergency Decree on the Digital Asset Businesses 2018, the Emergency Decree on the Amendment of the Revenue Code (No.19) 2018, and eleven SEC's regulations for Initial Coin Offerings in 2018, Cybersecurity Act 2019, Personal Data Protection Act 2019, and Digital Government Administration and Services Act 2019) are promulgated by related agencies for coping with the emerging of disruptive technologies such as cryptocurrency, net states, deep webs and dark webs. However, there is no study about Thai citizens and their roles in national security of Thailand under digital settings in Thailand. Therefore, the objective in this study is to investigate the state of art of Thai citizens and their roles in national security of Thailand.

Methodology

Documentary research with secondary data from various sources such as textbooks and online materials was employed in this study.

Reviews of Literature

Literature reviews were conducted in the following topics – state and sovereignty, civil disobedience, paradigm of Public Administration, Public Administration and products and services provision, net states, cryptocurrency, deep webs and dark webs, key citizen-related laws under digital setting in Thailand.

State and Sovereignty

States were important actors as sovereigns in modern sense since Treaty of Westphalia on October 24, 1648 (Treaty of Westphalia, 1648). However, its scope was clearly defined in the Convention on Rights and Duties of States (inter-American) on December 26, 1933 in Article one as follows a permanent population, a defined territory, government, and capacity to enter into relations with the other states (sovereignty) (Convention on Rights and Duties of States, 1933). State as a sovereign according to Article eight of the Convention had its legitimate power to run its internal and external affairs.

Civil Disobedience

Civil disobedience, firstly introduced by Henry David Thoreau in 1949, was the standard deviation of good citizen for any state. In general, according to a set of master pieces such as Henry David Thoreau (1949), Walzer (1967), Rawls (1999), the focus of civil disobedience was on individual with political intentions, called political civil disobedience. Though state had its absolute power to manage all affairs in state jurisdiction, individual as conscientious objector had a rights via a variety of non-violence affairs to express disagreement and show opposition to unjust government's policy or law in order to push for changing that policy or law. In addition, individual objector must get legal consequence from his/her action (Thoreau, 1949; Walzer, 1967; Rawls, 1999; Zain and Yusoff, 2017). However,

there was also another objection with economic incentives by employer(s), called business civil disobedience. This perspective of objection was introduced by Daniel Ostas in 2010. Its intention was for increasing profit and lessening cost of business with a variety of non-violent actions such as employment of illegal workers, violation of safety regulations on sprinklers and helmets in construction firms, and delegitimation of sound-insane public policy in snail-darter case during the construction of the Tellico Dam in eastern Tennessee (Ostas, 2010).

Paradigm of Public Administration

There were many scholars who employs paradigm as age for classifying all changes in Public Administration. However, this paper used only two paradigms – Nicholas Henry's paradigm as one of the most well-known paradigm in this field of study and my paradigm in 2018 as paradigm for both state and non-state actors.

The first paradigm comprised six paradigms as follows: paradigm 1 – the politics/administration dichotomy (1900 – 1926), paradigm 2 – principles of Public Administration (1927 – 1937), paradigm 3 – Public Administration as Political Sciences (1950 – 1970), paradigm 4 – Public Administration as Management (1950 – 1970), paradigm 5 – Public Administration as Public Administration (1970 – present), and paradigm 6 – governance (1990 – present). The last paradigm was very important because it strongly related to state minimalism and governance or network management among public sector, private sector, and people sector. Individuals and communities could play important roles in this paradigm (Henry, 2013).

The latter one is my paradigm in 2018. It consisted two sub-paradigms as follows: state-based paradigm and stateless-based paradigm. The state-based paradigm consisted of all topics under state's sovereignty in conventional Public Administration according to Nicholas Henry's paradigm such as e-government, digital weapon, New Public Management (NPM), communitarianism and civil society, bureaucracy

and its reform, government-based cryptocurrencies, and so on. In contrary to the state-based paradigm, the stateless-based paradigm was another story by focusing on all affairs of citizens beyond state's jurisdiction such as cryptocurrency and blockchain, deep web and dark web, and so on (Gohwong, 2018a, 2018b, 2019a).

Public Administration and Products and Services Provision

Public Administration according to Leonard D. White had its scope of products and services provision for the purpose of the state such as healthcare, economy, wasteland reclamation, education, public welfare, and religion (White, 1926). However, the agencies that provided public goods and services could be public agencies, firms, voluntary and non-profit organizations (VNPOs) or non-governmental organizations (NGOs), and cooperation among these organizations (Marini, 1971, Frederickson, 1989, Osborne and Gaebler, 1992; Peters, 2001; Osborne, 2003; O'Leary, Van Slyke, Kim, 2010; Daglio, Gerson, Kitchen, 2014; United Nations Economic Commission for Europe. 2017).

Net States

Net states were introduced by Alexis Wichowski since 2017. Net states were as digital non-state actors that comprised giant tech companies, such as Facebook, Google, Amazon, Apple, Microsoft, and Tesla. They had four key characteristics in their products and services as follows: international domain, technology orientation, strong influence on people's belief, and active expansion to provision of public goods and services. Their products and services, therefore, could have both positive and negative effects on sovereignty of the state. For positive side, net states provided public goods and services for supporting public sector. For example, Powerpacks, battery with solar cell, by Tesla and Google's Internet Project Loon were two net states that give infrastructure-related services – energy via batteries and communication via

Internet –to citizens in Puerto Rico after Hurricane Maria in 2017. In addition, net states promoted good governance via social media.

On contrary to positive side, net states could do their own affairs arbitrarily beyond states' jurisdiction. For instance, Project Natick of Microsoft since 2015 was self-contained data centers, with 864 servers and 27.6 petabytes of storage, beyond states' jurisdiction, sunk in the ocean near Scotland's Orkney Islands beyond 12 miles offshore according to the United Nations Convention on the Law of Sea (UNCLOS). It was not only cost reduction for electricity and overheating prevention, but also non-compliance with states' laws and regulations as business civil disobedience. Furthermore, Microsoft used to deny FBI's request for data disclosure of its email user because the emails were not in US territory. This example, Microsoft protect its user from states' laws and mandates. Another instance, data brokers like Acxiom, Nielsen, Experian, Equifax, and CoreLogic bought and sold citizen's data to third parties. In addition, net states created models of individual citizen by their data. For example, Gmail scanned all contents of your personal email for showing banners in your email account and advertisement (Roach, 2018; Warren, 2018; Wichowski, 2020).

Cryptocurrency

Cryptocurrency was a code-based money with third party-free characteristics. Bitcoin, Ethereum, Ethereum Classic, Ripple, and Monero were well-known examples of this currency. The materials of this digital money was electromagnetic. Its core technologies were programming (such as C++, Go, Python, Java, Rust, Solidity, WebAssembly, C, Haskell, Javascript / Node.js), blockchain, and cryptography with its supportive technologies (such as IoT, AI, cloud computing). According to Srirath Gohwong's studies during 2018 – 2020, there were three types of cryptocurrency as follows: non-governmental cryptocurrency, government-based cryptocurrency, and quantum-based cryptocurrency (Gohwong, 2017, 2018a, 2018b, 2019b, 2020). However, only non-

governmental cryptocurrency was reviewed here due to its importance on Thais' role – both supporting and objection.

Non-governmental cryptocurrency was the most well-known currency for everyone. It comprised two key groups – public-based cryptocurrency and privacy-based cryptocurrency. The first group could trace all information of money such as sender, receiver, and the amount of money. Bitcoin (BTC), Ethereum (ETH), Ripple (XRP), Bitcoin Cash (BCH), Litecoin (LTC), Stellar (XLM), and Ethereum Classic (ETC) were examples of the first group. For Thailand, buying and selling cryptocurrency were legal in the era of General Prayuth Chan-o-cha's government according to the Emergency Decree on the Digital Asset Businesses B.E. 2561 (A.D. 2018)", "the Emergency Decree on the Amendment of the Revenue Code (No.19) B.E. 2561 (A.D. 2018)", and eleven SEC's regulations for Initial Coin Offerings in 2018 with only seven legalized cryptocurrencies as follows: Bitcoin, Ethereum, Ripple, Bitcoin Cash, Litecoin, Stellar, and Ethereum Classic. On contrary to the first group, the latter group could hide all aforementioned information by CryptoNote and CryptoNight. Bytecoin (BCN), Verge (XVG), Zcash (ZEC), Zcoin (XZC), Monero (XMR), MoneroC (CXMR), Monero Gold (XMRG), MoneroV (XMV), Monero Classic (XMC), Monero-Classic (XMC), Monero 0 or Monero Zero (XMZ / ZMR), and Monero Original (old Monero) (XMO) were examples of the latter group. Therefore, Thais could use their own considerations for doing their own affairs beyond Thai government's jurisdiction (Gohwong, 2017, 2018a).

Deep Webs and Dark Webs

Deep webs and dark webs as underground web sites were direct threats to sovereignty of every state because they were 96% of total web sites beyond states' jurisdiction whereas the rest were surface webs or normal web sites in everyday life. Deep webs were dedicated to two objectives - (1) to use for internal lawful affairs of general organization, and (2) to use for illegal affairs

(such as drugs, weapons, contract killing, fraud such as cloned credit card, hacking, and pornography). Dark webs were subset of deep webs for illegal affairs only, approximately 3% of total deep webs. They both could not be accessible by conventional search engines and commonly-used web browsers (such as Microsoft Edge, Mozilla Firefox, Opera, Google Chrome). TOR and I2P were two examples of special web browsers for deep webs and dark webs. In addition, they could be used by cybercriminals with privacy-based cryptocurrencies to do stateless-based illegal affairs beyond states' jurisdiction (Gohwong, 2018a, 2019a).

Key Citizen-related laws under digital setting in Thailand

There were key citizen – related laws under digital setting in Thailand as follows: Constitution of the Kingdom of Thailand 2017, National Security Council Act 2016, Ministry Enhancing Act (Book no.17) 2016 (Establishing the Ministry of Digital Economy and Society), Computer-related Crime Act (No.2) 2017, Cybersecurity Act 2019, Personal Data Protection Act 2019, and Digital Government Administration and Services Act 2019.

Constitution of the Kingdom of Thailand 2017

Thailand was the same as every country in the world by using constitution as highest law for determining the scope of national security and guaranteeing human rights and liberties under rule of law. The latest constitution was the twentieth constitution that enacted on April 6, 2017.

For the first intention of Constitution, national security of Thailand was not a new issue in Constitution of Thailand. In fact, it was determined in all Constitutions by the drafters as follows: monarchical institution, democratic regime of government with the King as Head of State, independence, sovereignty, territorial integrity, economic security, martial security, religious institution, public safety and order, and readiness of country to handle all forms of threat (Interim Charter for the Administration of Siam

Act 1932, Constitution of the Kingdom of Siam 1932, Constitution of the Kingdom of Thailand 1946, Constitution of the Kingdom of Thailand (Interim) 1947, Constitution of the Kingdom of Thailand 1949, Constitution of the Kingdom of Thailand 1932 (Revised 1952), Interim Charter for the Administration of the Kingdom 1959, Constitution of the Kingdom of Thailand 1968, Interim Charter for Administration of the Kingdom 1972, Constitution for the Administration of the Kingdom 1974, Constitution for Administration of the Kingdom 1976, Interim Charter for Administration of the Kingdom 1977, Constitution of the Kingdom of Thailand 1978, Interim Charter for Administration of the Kingdom 1991, Constitution of the Kingdom of Thailand 1991, Constitution of the Kingdom of Thailand 1997, Constitution of the Kingdom of Thailand (Interim) 2006, Constitution of the Kingdom of Thailand 2007, Constitution of the Kingdom of Thailand (Interim) 2014, Constitution of the Kingdom of Thailand 2017).

For the latter intention, it guaranteed individual rights and liberties of Thais except the necessity of public interest under related laws, especially the lawful use of personal data (Section 32), freedom of opinions expression in speech, writing, and printing or any other means (Section 34), freedom of communication by any means (Section 36), accessibility of public data and public agency data according to law, petition submission to public agencies and prosecution of public agencies for liability (Section 41), Freedom of establishment of any association, co-operative, union, organization, community, or any other group (Section 42), a joint petition submission by individuals and a community to public agencies for proposing recommendations or refraining from action (Section 43), and freedom of peaceful assembly (Section 44) (Constitution of the Kingdom of Thailand 2017).

National Security Council Act 2016

National Security Council Act 2016 was the law that defined the current definition of National security of Thailand as the state of being free from

any threat to Thailand in the following issues: independence, sovereignty, territorial integrity, religious institution, monarchical institution, public safety, peaceful livelihood, national interests, and democratic regime of government with the King as Head of State. In addition, it was also the readiness of country to handle all forms of threat (National Security Council Act 2016).

Ministry Enhancing Act (Book no.17) 2016 (Establishing the Ministry of Digital Economy and Society)

The Ministry of Digital Economy and Society (MDES) oversaw IT-related affairs of Ministry of Information and Communication Technology (MICT) by Ministry Enhancing Act (Book no.17) 2016 (Establishing the Ministry of Digital Economy and Society). It consisted of five dependent agencies (Office of the Minister, Office of the Permanent Secretariat, Meteorological Department, Office of the National Digital Economy and Society Commission (ONDE), National Statistical Office (NSO), three dependent public firms (TOT Public Company, Ltd (TOT), CAT Telecom Public Company, Ltd (CAT), Thailand Post Company, Ltd, and two public organizations (Electronic Transactions Development Agency (ETDA), Digital Economy Promotion Agency (DEPA)) (Ministry Enhancing Act (Book no.17) 2016).

Computer-related Crime Act (No.2) 2017

It was the amendment of Computer-related Crimes Act 2007 in 2017 with key issues as follows: (1) Ministry of Digital Economy and Society was in charge of computer-related crime, (2) computer-related crime consists of offences as follows: dissemination of abusive content (such as spam, harassment, child/sexual/violence), the use of malicious code (Virus, Worm, Trojan, Backdoor, Spyware), illegal collection of information (scanning, sniffing, social engineering), hacking and intrusion (such as Privileged Account Compromise, Unprivileged Account Compromise, Application Compromise), unavailability of computer and its network system (DoS, DDoS, sabotage), lack of integrity of

information (unauthorized access to information, unauthorized modification of information), and fraud (unauthorized use of resources, Copyright infringement, Masquerade or identity theft) (European Computer Security Incident Response Team Network, 2003; Computer-related Crime Act (No.2) 2017).

Cybersecurity Act 2019

Cybersecurity Act 2019 intention mainly focused on a defense of sovereignty, especially national security, economic security, martial security, and public order, from both external and internal cyber-attacks via management of Critical Information Infrastructure organizations (CII organizations). There were a set of related agencies at different level of administration as follows: strategic (such as National Cyber Security Committee (NCSC), MDES, authorized court, Office of the National Cybersecurity Committee for providing academic job and routine jobs of NCSC and the CRC), middle (such as Cybersecurity Regulating Committee (CRC), authorized court), and operational (Supervising organization, CII, Committee Managing the Office of the National Cybersecurity Committee (CMO), National Security Council). Cyber-attacks were determined by NCSC in three levels – non-critical level, critical level, and crisis level. Penalty were maximum fine and/or imprisonment, based on violation of confidentiality, integrity, and availability of data (Cybersecurity Act 2019; Gohwong, 2019c).

Personal Data Protection Act 2019

This act was promulgated in the Government Gazette on May 27, 2019 under the pressure from the application of General Data Protection Regulation (EU GDPR) 2016/679 on May 25, 2018 in order to enhance data governance, especially data security, data privacy, transparency of data use. There were key issues in this Act as follows: (1) it protected rights of citizens as data subjects. Personal data of citizens stood for any personal data for both direct and indirect person identification, except data of the

death, (2) data collection, data storage, data security, disclosure, and dissemination, data application and data transferring between agencies in public, private, and people sector were key activities in this Act, (3) data owner must provide consent to the collection, use and disclosure of personal data only for the purposes specified by the user collection. In addition, the data owner had rights to withdraw consent and request to delete or destroy data at any time, (4) all related agencies that did all aforementioned activities were two types – data controller and data processor, both inside and outside of Thailand. Data controller was a person or a juristic person with decision-making power about personal data's collection, use, and disclosure. Data processor was a person or a juristic person who did personal data's collection, use, and disclosure, both direct implementer and agent on behalf of data controller. Data processor was not data controller. Data processor must maintain data security, especially integrity and confidentiality, and (5) this enforcement of the Act was postpone in Chapter 2, 3, 5, 6, 7 and Section 95 to 31 May 2021 on May 20, 2020 by the Royal Decree on determination of agencies and businesses that data controllers are not subject to Personal Data Protection Act 2019 2020 (Personal Data Protection Act 2019; Herveg, 2019; Royal Decree on determination of agencies and businesses that data controllers are not subject to Personal Data Protection Act 2019 2020)

Digital Government Administration and Services Act 2019

The act is well-known for general people as Digital Government Act. It mainly focused on data governance in the Thai public sector that promote standardized data management of public agencies sector in Thailand in eight activities – data acquisition, data storage, data classification, data processing, data cleaning, data security, disclosure, and dissemination, data application, data deletion and erasure (Digital Government Administration and Services Act 2019).

Finding

National security of Thailand could be defined by employing three key laws – Constitution of the Kingdom of Thailand 2017, National Security Council Act 2016 and Cybersecurity Act 2019 as the state of being free from any threat, both online and offline, to Thailand in the following issues: independence, sovereignty, territorial integrity, economic security, martial security, religious institution, monarchical institution, public safety and order, and democratic regime of government with the King as Head of State. In addition, it was also the readiness of country to handle all forms of threat (Constitution of the Kingdom of Thailand 2017; National Security Council Act 2016; Cybersecurity Act 2019). According to this definition, Thai citizens had a big role as both supporters and objectors to national security of Thailand.

As supporters, Thai citizens were under twenty-two promulgated laws for enhancing digital economy and data governance in Thai public sector as follows: Constitution of the Kingdom of Thailand 2017, National Security Council Act 2016, Ministry Enhancing Act (Book no.17) 2016 (Establishing the Ministry of Digital Economy and Society), Computer-related Crime Act (No.2) 2017, the Emergency Decree on the Digital Asset Businesses 2018, the Emergency Decree on the Amendment of the Revenue Code (No.19) 2018, eleven SEC's regulations for Initial Coin Offerings in 2018, Cybersecurity Act 2019, Personal Data Protection Act 2019, Digital Government Administration and Services Act 2019, and Royal Decree on determination of agencies and businesses that data controllers are not subject to Personal Data Protection Act 2019 2020. Good Thai citizens had their individual rights and liberties according to these laws except the necessity of public interest under related laws. They complied with government's public policies such as tax payment, in the surface web sites, accessed by commonly used web browsers like Microsoft Edge, Mozilla Firefox, Google Chrome, Opera and so on, that were easily monitored by Thai government. Thai citizens were treated as

citizen-user whom Thai public agencies provided public goods and services with efficiency, effectiveness, and economy due to strong influence of New Public Management (NPM) in Thai public reform. Unfortunately, this supporters-oriented role of Thai citizens had very little impact with national security because the size of surface web sites was only 4% of total web sites.

For example, Thai citizens inevitably used Thai Baht as national currency, both cash and cashless form (such as debit cards, credit cards, telephone banking, Internet banking, Bank of Thailand Automated High-value Transfer Network (BAHTNET), PromptPay), to do any transaction in all of their financial activities under easily monitoring and controlling of many third-parties such as Ministry of Finance (MOF), Bank of Thailand (BOT), commercial banks, financial institutions. MOF and BOT officially monitored and controlled all money-related affairs in Thailand (such as money supply, money transfer) by using various mechanisms of monetary policy, fiscal policy, and government-based IT. Therefore, Thai government could respond to any illegal affair as threat against national security such as tax evasion, money laundering, terrorism financing, fraud in investment, bribery and corruption, drug trafficking, and human trafficking.

However, on contrary to the supporters-oriented role, Thai citizens could become high-impact objectors to national security due to the emerging of external changes with net states, non-governmental cryptocurrency (such as Bitcoin (BTC), Ethereum (ETH), Ripple (XRP), Bitcoin Cash (BCH), Litecoin (LTC), Stellar (XLM), and Ethereum Classic (ETC), Monero (XMR) – a key privacy-based cryptocurrency for profiting, cryptojacking or illegal mining, and illegal money transfer), deep webs and dark webs with 96% of web sites, accessed by underground web browsers such as TOR and I2P. The anti-state role would be presented as follows:

First, the most popular underground web browsers in Thailand was TOR with

approximately 2,656,342 nodes or users according to Tor Metrics' data on 2 July 2020, including relay users and bridge users (Tor Metrics, 2020a, 2020b), or 5.1% of total Thai internet subscriber of 2020, 52,000,000 subscribers (Kemp, 2020). For I2P, its users in Thailand according to I2P Metrics' data on 2 July 2020 was 85 routers (I2P Metrics, 2020), or .0002% of total mentioned Thai internet subscriber of 2020.

Second, non-governmental cryptocurrency allowed Thai citizens to easily disobey Thai government for illegal affairs (such as organized crime, terrorist financing, tax evasion, and cryptojacking or illegal mining) without Thai government's monitoring and controlling because Thai citizens could easily hide their identities, data about money transfer (such as amount, sender and receiver) by using privacy-based cryptocurrency such as Monero (XMR), Zcash (ZEC), and Zcoin (XZC). For example, 83 Thais from 2,055 Thai respondents according to the survey of Siam Blockchain during 5 – 12 July 2017 employed Monero (17 Thais), Zcash (62 Thais), and Zcoin (4 Thais) for making profits (Siam Blockchain, 2017). Furthermore, they could be much more anonymous when they employed privacy-based cryptocurrency with web browsers for underground web sites. For instance, according to the data of Unit 42 – a global threat intelligence team at Palo Alto Networks, XMRig miner, a modified open sourced Monero CPU Miner for illegal Monero mining, was downloaded by cyber-criminals from Thailand for making Profit from cryptojacking more than 3,545,437 times during October 2017 – January 2018 as ranked number one, almost doubled in number two – Vietnam 1,830,065 times. This cryptojacking employed XMRig mining software via VBS files and BITSAdmin for downloading scripts and XMRig mining tool from a remote location, XMRig proxy services for hiding the ultimate mining pool destination, and Nicehash – a well-known marketplace for buying and selling hashing processing power (Grunzweig, 2018; Gohwong, 2019d),

Last, net states like Microsoft, Google, Facebook, and Amazon challenged Thailand's sovereignty by intervening in the public service provision of Thai government, both economic and social affairs, and protecting their Thai citizens as their citizen-user from Thai government. The first issue on Thai public service provision was presented as follows:

For Microsoft, it played an important role in public service provision of Thailand via its social programs and economic stimulus programs. For instance, Microsoft provided its social programs in 2020 such as financial service provision to Thai farmers affected by CoV19 through cooperation among Thailand's Bank of Agriculture and Agricultural Cooperatives (BAAC), Microsoft Thailand, and Bluebik Group via <https://agri.baac.or.th/> website and app; data management of on public restrooms hygiene by using a mobile app and Microsoft AI and Cognitive Services through cooperation between Thailand's Ministry of Public Health and Microsoft Thailand for identifying public health risks and notifying local restroom operations staffs to improve sanitation conditions; online learning during COVID-19 pandemic via Microsoft Teams for Education for 150 Thai universities through cooperation between Ministry of Higher Education, Science, Research and Innovation and Microsoft Thailand. Another instance, Microsoft provided its economic stimulus programs in 2020 such as "Hack the Future: Business Rebound Edition" project was an economic stimulus program through cooperation between Microsoft Thailand and RISE, Southeast Asia Regional Enterprise Innovation Accelerator for increasing competitive edges of Thai SME entrepreneurs by finding the best three startups, each of three problems – manufacturing sectors and IoT-related business groups, retail industry and restaurant service, medical service and tourism, to bring their solutions on Microsoft Azure cloud platform to market together with Microsoft; AI lab for farming sector and the smart city project to startups, universities and R&D organizations in accessibility of Microsoft research lab and a

digital platform through cooperation between Microsoft Thailand and MDES (Microsoft, 2019, 2020a, 2020b, 2020c; Samejaidee, 2019).

For Google, it had an important role in public service provision of Thailand via its social programs and economic stimulus programs. Since 2018, Google implemented its “Leave No Thais Behind” strategy under “Google for Thailand” project in four areas since 2018 as follows: “Google Station” as its high-speed public WiFi through a partnership with CAT Telecom for increasing internet access, “Google Space” as its digital skills training facility in Bangkok with its partner – True Digital Park, “YouTube Pop-Up Space” in Bangkok in order to localize content and local products according to the needs of Thais, and Google My Business, a free business listing on Google Search and Google Maps, for supporting Thai SMEs and startups to grow efficiently with a collaboration with Siam Commercial Bank. In addition, in 2019, Google expanded its scope of AI-related research in diabetic retinopathy screening through cooperation with Department of Medical Services, Ministry of Public Health. The enlargement was to increase the number of clinics from 1 to 8 clinics, including Bangkok, Pathum Thani and Chiang Mai (Tortermvasana, 2018; Manager Online, 2019).

For Facebook, it had an important role in public service provision for strengthening society and economy of Thailand. For instance of social issue, Facebook offered Thais to create their own groups for sharing mutual interests and building a strong online community, at least one million groups. “Help Us Read Thai community” for visually impaired or blind people, “Run2gether” for disabilities and normal people, and “HandUp Network” with more than 5,000 volunteers in professional fields for supports non-profit organizations were three dedicated groups for strengthening Thai society. Another instance of economic issue, Live feature and Marketplace feature, developed from Live feature, were Facebook products in order to promote e-Commerce for Thai SMEs (Areeperphon, 2018).

For Amazon, it also had an important role in public service provision for society and economy of Thailand through EdStart global program, run by its own company - Amazon Web Services (AWS). AWS joined with OpenDurian, abbreviate from Open-Du (Thai word for watch in English) - rian (Thai word for study in English), a Thai local startup (EdTech) for making a cloud-based platform for learning and test-preparation (such as English language test, General Aptitude Test (GAT), Professional and Academic Aptitude Test in Mathematics (PAT1), SAT, Chulalongkorn University Academic Aptitude Test (CU-AAT), Scholastic Management Aptitude Requirement Test – I (SMART-I) for admission to a bachelor's degree in accounting and business administration of Thammasat University, Doctor Aptitude Test, biology and mathematics) to serve three million users in Thailand, including students and working people. In addition, this startup also offered some free exam for helping students (OpenDurian, 2017; Toomgum, 2019).

In addition, the latter issue on the user protection of Microsoft, Google, and Facebook was found that they hardly protect their users by often obeying Thai laws as follows:

For Microsoft, it did not protect its Thai users by revealing its user's sensitive data under valid legal orders to Thai government. For example, Microsoft gave IP addresses related to the email account of a Thai stockbroker for convicting the offender in charge of dissemination of erroneous information with negative impact on Thailand's stock exchange during the trial in 2014. Privacy International also revealed that Microsoft was the only company that included the Thai government's root CA in its list of trusted certificates for digital certification (Privacy International, 2017a, 2017b). In addition, Microsoft also supported Thailand's Department of Special Investigation (DSI) through its Microsoft SQL Server 2012 (an enterprise data management software) and Apache Hadoop (an open-source software for distributed storage and big data management) for manage big data with

automated notification of any suspicious persons or activities (Vietnam Investment Review, 2014). For Google, it usually obeyed Thai law by removing all or part of the content on Google service in response to valid legal requests from the Thai government. However, Google sometimes did not remove contents in response to valid legal requests from the Thai government agencies (such as MDES) or Thai individual (such as a member of Royal Thai Parliament). The total requests since 2009 were 964 whereas total items for removal since 2009 were 27,233. The content that Google was asked to remove was disseminated by YouTube the most with 892 requests (92.5%). The reason for removal was government criticism the most with 917 requests (95.1%) (Google, 2019). For Facebook, it did only content access restrictions, not provision of account information or content of any Facebook user to Thai government. Facebook mostly limited access to content based on Computer-related Crimes Act 2007 and Computer-related Crime Act (No.2) 2017 in response to valid legal requests from the Thai government. According to Facebook's data since 2013, the total requests were 164 whereas total restricted access items were 2,780. The reason for restricted access items was mostly on defamation in violation of Thailand's Penal Code Section 112 (lèse-majesté) and Section 14(3) of the Computer Crimes Act (The Nations, 2016; Facebook, 2020a, 2020b).

Discussion

National security was an important aspect of sovereignty. It needed the strong cooperation between Thai government and citizens. As good citizens as supporters of Thai government's jurisdiction, citizens must comply with all laws. However, the growth in the number of IT-related laws in Thailand, such as Computer-related Crime Act (No.2) 2017, Ministry Enhancing Act (Book no.17) 2016 (Establishing the Ministry of Digital Economy and Society), Cybersecurity Act 2019, Personal Data Protection Act 2019, and Digital Government Administration and Services Act 2019, reflected the increased digital control of

citizens by the Thai government. For example, Thailand was one of three countries, along with Singapore and Vietnam, in ASEAN who enacted Cybersecurity Act for effectively coping with cyber-attacks. These laws were not only enhancement of national security, protection of rights, protection, and remedy of cyber-attacks, but also controlling of money supply and transactions in Thailand. For enhancement of national security, protection of rights, protection and remedy of cyber-attacks, the enforcement of these IT-related laws allowed MDES and related authorized agencies that increased the level of controlling on data via surface web sites because data were monitored and controlled in every processes in public agencies by data governance and personal data protection. In addition, data accessibility by Thai governments to IT devices and computer systems of non-government sectors could be easily done by NCSC's violence assessment of cyber-attacks. For example, NCSC might assign Secretary General of NCSC to do all necessary measures for protection and remedy of cyber-attacks without court's order in the crisis level. In addition, Thai government and Bank of Thailand (BOT) used both cash and cashless fiat currency (such as debit card, credit card, BAHTNET, and PromptPay) and Inthanon as Thai government-based cryptocurrency for controlling of money supply and transactions. Money is one of the most important resources in state administration because Thai government use money for providing public goods and services and controlling money supply and money transfer in order to achieve sustainable growth economy with cybersecurity.

However, though many Thai citizens were good supporters of Thai government, Thai citizens had another alternative by using disruptive technologies for doing their stateless-oriented activities. These objectors, then, became direct severe threats against national security and sovereignty of Thailand because they committed civil disobedience-oriented activities beyond Thai government's jurisdiction. State monopoly in the provision of public goods and services obviously

became an outdated public policy of Thai government. Thai citizens could hide all data of their identities and money transfer by using web browsers for underground web sites or privacy-based cryptocurrency. For the use of TOR, I2P, and privacy-based cryptocurrency (Siam Blockchain, 2017, I2P Metrics, 2020, Tor Metrics, 2020a, 2020b), though the number of users was quite small – 2,656,342 TOR's users (5.1% of total Thai internet subscriber of 2020), 85 I2P's users (.0002% of total Thai internet subscriber of 2020), and 83 Thais (4% of total respondents according to the Siam Blockchain's survey in 2017), it should be noted here that it was the beginning of stateless-oriented affairs in Thailand. These affairs implied that Thai government had no absolute capability to control both its own internal and external affairs anymore. A small number of Thais could do their own affairs arbitrarily beyond Thai government's jurisdiction. For example, Thais directly did peer-to-peer money transfer by themselves without BOT as third party by using Monero, Zcash, and Zcoin (Siam Blockchain, 2017; Gohwong, 2018b). Another example, tax payment became consideration of Thai citizens due to anonymous state of Monero, Zcash, and Zcoin, not a determined duty in the Section 50 of Constitution of Thailand 2017 anymore (Constitution of the Kingdom of Thailand 2017; Gohwong, 2018b).

In addition, Thai citizens were not only Thai citizen-user, but also net states' citizen-user. On contrary to Thais as citizen-user of state, online habits of Thai citizens as net states' citizen-user (such as post, like, tweet, web site visiting, search, shopping) directly affected the provision of goods and services by net states because these online habits were citizen-user' votes for desired goods and services of net states. Therefore, net states sometimes did not comply with Thai laws in order to protect Thai citizens as their citizen-user as a business civil disobedience. For example, Google sometimes did not remove contents in response to valid legal requests from MDES and a member of Royal Thai Parliament (Google, 2019). Another example was Facebook who did not provide

account information or content of any Facebook user to Thai government. Facebook did only content access blocking for Thai users (The Nations, 2016; Facebook, 2020a, 2020b).

In addition, Microsoft, Google, Facebook, and Amazon cooperated with Thai public agencies in public service provision via their social programs (such as Microsoft Thailand's financial service provision to Thai farmers affected by CoV19, data management for clean public restrooms, online learning during COVID-19 via Microsoft Teams for 150 Thai universities (Microsoft, 2019, 2020a, 2020b); Google Station, Google Space, and AI-related research in diabetic retinopathy screening (Tortermvasana, 2018; Manager Online, 2019); Facebook's online community (Areeperphon, 2018); Amazon cooperation with OpenDurian (OpenDurian, 2017; Toomgum, 2019)) and economic stimulus programs (such as Microsoft's Hack the Future: Business Rebound Edition project, AI lab for farming sector and the smart city project (Samejaidee, 2019; Microsoft, 2020c); Google's YouTube Pop-Up Space and Google My Business (Tortermvasana, 2018); Facebook's Live feature and Marketplace feature (Areeperphon, 2018); Amazon cooperation with OpenDurian (OpenDurian, 2017; Toomgum, 2019)). These projects made net states influence Thai government, Thai firms, and Thai society by increasing switching cost for their users. These users would encounter significant difficulties when switching from one product/service to another because user acquaintance, software maintenance, and software update increase level of dependency on Microsoft.

In conclusion, the findings of Thais as supporters and objectors of Thai government revealed the starting point of paradigm shift in Public Administration from state-based Public Administration to stateless-based Public Administration (Gohwong, 2018b). For state-based Public Administration, partnership among public, private, and people sector was still an important mechanism for public service provision in Thailand. However, Thai government did not have absolute power for managing all affairs

under its jurisdiction anymore due to the emerging of net states. For example, Thai government must make requests to Google (for removing all or part of the content on Google services) and Facebook (for blocking content access). In addition, Thai government depended on net states with its cooperation with these giant tech companies. For example, DSI used Microsoft SQL Server 2012 for automated notification of any suspicious persons or activities. On contrary to state-based Public Administration, stateless-based Public Administration gradually decrease Thai government's absolute power on its affairs by the emerging of cryptocurrency and underground web sites and browsers. Legal compliance of Thais (such as money transfer, buying and selling cryptocurrency) sometimes was under their consideration.

Conclusion

Nowadays Thai citizens has a big role as both supporters and objectors for national security of Thailand due to both external and internal settings. They are treated by both Thai government and net states as citizen-user with different treatment. Thai government treats citizen-user as client whereas net states treat citizen-user as both voter and client.

References

- [1] Areeperphon, P. 2018. **Open a new home. Facebook Thailand. Thai people use 51 million people per month. Chat with the top 5 sellers in the world.** Retrieved from <https://thestandard.co/facebook-thailand/> [In Thai]
- [2] **Computer-related Crime Act (No.2) 2017.** Retrieved from <http://www.ratchakitcha.soc.go.th/DATA/PDF/2560/A/010/24.PDF> [In Thai]
- [3] **Constitution of the Kingdom of Siam 1932.** Retrieved From <http://www.ratchakitcha.soc.go.th/DATA/PDF/2475/A/529.PDF> [In Thai]
- [4] **Constitution of the Kingdom of Thailand 1946.** Retrieved From <http://www.ratchakitcha.soc.go.th/DATA/PDF/2489/A/030/318.PDF> [In Thai]
- [5] **Constitution of the Kingdom of Thailand (Interim) 1947.** Retrieved From https://www.parliament.go.th/ewtadmin/ewt/parliament_parcy/ewt_dl_link.php?nid=7227&filename=index [In Thai]
- [6] **Constitution of the Kingdom of Thailand 1949.** Retrieved From https://www.parliament.go.th/ewtadmin/ewt/parliament_parcy/ewt_dl_link.php?nid=7223&filename=index [In Thai]
- [7] **Constitution of the Kingdom of Thailand 1932 (Revised 1952).** Retrieved From https://www.parliament.go.th/ewtadmin/ewt/parliament_parcy/ewt_dl_link.php?nid=7221&filename=index [In Thai]
- [8] **Constitution of the Kingdom of Thailand 1968.** Retrieved From https://www.parliament.go.th/ewtadmin/ewt/parliament_parcy/ewt_dl_link.php?nid=7218&filename=index [In Thai]
- [9] **Constitution for the Administration of the Kingdom 1974.** Retrieved From https://www.parliament.go.th/ewtadmin/ewt/parliament_parcy/ewt_dl_link.php?nid=7214&filename=index [In Thai]
- [10] **Constitution for Administration of the Kingdom 1976.** Retrieved From https://www.parliament.go.th/ewtadmin/ewt/parliament_parcy/ewt_dl_link.php?nid=7212&filename=index [In Thai]
- [11] **Constitution of the Kingdom of Thailand 1978.** Retrieved From https://www.parliament.go.th/ewtadmin/ewt/parliament_parcy/ewt_dl_link.php?nid=7210&filename=index [In Thai]
- [12] **Constitution of the Kingdom of Thailand 1991.** Retrieved From https://www.parliament.go.th/ewtadmin/ewt/parliament_parcy/ewt_dl_link.php?nid=7206&filename=index [In Thai]
- [13] **Constitution of the Kingdom of Thailand 1997.** Retrieved From

- <http://www.ratchakitcha.soc.go.th/DATA/PDF/2540/A/055/1.PDF> [In Thai]
- [14] **Constitution of the Kingdom of Thailand (Interim) 2006**. Retrieved From https://www.parliament.go.th/ewtadmin/ewt/parliament_parcy/ewt_dl_link.php?nid=7197&filename=index [In Thai]
- [15] **Constitution of the Kingdom of Thailand 2007**. Retrieved From <https://www.ombudsman.go.th/10/documents/law/Constitution2550.pdf> [In Thai]
- [16] **Constitution of the Kingdom of Thailand (Interim) 2014**. Retrieved From <http://www.ratchakitcha.soc.go.th/DATA/PDF/2557/A/055/1.PDF> [In Thai]
- [17] **Constitution of the Kingdom of Thailand 2017**. Retrieved From <http://www.ratchakitcha.soc.go.th/DATA/PDF/2560/A/040/1.PDF> [In Thai]
- [18] **Convention on Rights and Duties of States (inter-American); December 26, 1933**. Retrieved from https://avalon.law.yale.edu/20th_century/intam03.asp
- [19] **Cybersecurity Act 2019**. Retrieved from http://www.ratchakitcha.soc.go.th/DATA/PDF/2562/A/069/T_0020.PDF [In Thai]
- [20] Daglio, M.; Gerson, D.; Kitchen, H. 2014. **Building Organisational Capacity for Public Sector Innovation**. Background Paper prepared for the OECD Conference “Innovating the Public Sector: from Ideas to Impact”, Paris, 12-13 November 2014.
- [21] **Digital Government Administration and Services Act 2019**. Retrieved from http://www.ratchakitcha.soc.go.th/DATA/PDF/2562/A/067/T_0057.PDF [In Thai]
- [22] European Computer Security Incident Response Team Network (eCSIRT). 2003. **WP4 Clearinghouse Policy-Release 1.2**. Retrieved from <http://www.ecsirt.net/cec/service/documents/wp4-clearinghouse-policy-v12.html>
- [23] Facebook. 2020a. **Government Requests for User Data**. Retrieved from <https://transparency.facebook.com/government-data-requests/>
- [24] Facebook. 2020b. **Content Restrictions Based on Local Law**. Retrieved from <https://transparency.facebook.com/content-restrictions>
- [25] Frederickson, H.G. 1989. **Minnowbrook II: Changing Epochs of Public Administration**. *Public Administration Review* 49(2): 95 - 100.
- [26] Gohwong, S. 2017. “The state of the art and trend of cashless society in Thailand” *Asian Political Science Review* 1 (2): 65-72.
- [27] Gohwong, S. 2018a. The State of the Art of Cryptocurrencies. *Asian Administration and Management Review* 1 (2): 1-16.
- [28] Gohwong, S. 2018b. **Paradigm of Public administration**. 13th National Graduate Conference at UNISERV Chiang Mai University during 24 – 25 December 2018. [In Thai]
- [29] Gohwong, S. 2019a. Deep Web: A Residual of e-Public Administration. *Asian Political Science Review* 3(1): 126 – 131.
- [30] Gohwong, S. 2019b. **Government-based Cryptocurrencies**. 8th International Social Sciences and Business Research Conference, Università della Svizzera italiana, Lugano, Switzerland on 20-23 May 2019.
- [31] Gohwong, S. 2019c. The State of the Art of Cybersecurity Law in ASEAN. *Journal of Crime, Law and Social Issues* 6(2): 12 – 23.
- [32] Gohwong, S. 2019d. The State of the Art of Cryptography-based Cyber-attacks. *Journal of Crime, Law and Social Issues* 6(2): 24 – 34.

- [33] Gohwong, S. 2020. **Quantum Cryptography-based Cryptocurrency**. 10th International Social Sciences and Business Research Conference, Università della Svizzera italiana, Lugano, Switzerland on 3 – 6 February 2020.
- [34] Google. 2019. **Government requests to remove content**. Retrieved from <https://storage.googleapis.com/transparencypreport/google-government-removals.zip>
- [35] Grunzweig, J. 2018. **Large Scale Monero Cryptocurrency Mining Operation using XMRig**. Retrieved from <https://unit42.paloaltonetworks.com/unit42-large-scale-monero-cryptocurrency-mining-operation-using-xmrig/>
- [36] Henry, N. 2013. **Public Administration and Public Affairs**. NY: Pearson.
- [37] Herveg, J. 2019. **TH – EU Seminar on eCommerce & GDPR GDPR Implications on Business**. TH-EU Seminar on E-Commerce and GDPR Anantara Siam Bangkok Hotel, Bangkok, Thailand on 6 June 2019.
- [38] **Interim Charter for the Administration of Siam Act 1932**. Retrieved From <http://www.ratchakitcha.soc.go.th/DATA/PDF/2475/A/166.PDF> [In Thai]
- [39] **Interim Charter for the Administration of the Kingdom 1959**. Retrieved From <http://www.ratchakitcha.soc.go.th/DATA/PDF/2502/A/017/1.PDF> [In Thai]
- [40] **Interim Charter for Administration of the Kingdom 1972**. Retrieved From https://www.parliament.go.th/ewtadmin/ewt/parliament_parcy/ewt_dl_link.php?nid=7217&filename=index [In Thai]
- [41] **Interim Charter for Administration of the Kingdom 1977**. Retrieved From https://www.parliament.go.th/ewtadmin/ewt/parliament_parcy/ewt_dl_link.php?nid=7211&filename=index [In Thai]
- [42] **Interim Charter for Administration of the Kingdom 1991**. Retrieved From https://www.parliament.go.th/ewtadmin/ewt/parliament_parcy/ewt_dl_link.php?nid=7207&filename=index [In Thai]
- [43] I2P Metrics. 2020. **Routers by country [Thailand]**. Retrieve from <https://i2p-metrics.np-tokumei.net/router-distribution>
- [44] Jermsittiparsert, K. & Sriyakul, T. (2014). The Development of Population Potential and National Power by Elevating the Professional Standard for Sport Coaches. **Asian Social Science**, 10(10), 188-198. DOI: 10.5539/ass.v10n10p188.
- [45] Kemp, S. 2020. **DIGITAL 2020: THAILAND**. Retrieve from <https://datareportal.com/reports/digital-2020-thailand>
- [46] Laudon, K.C. and Laudon, J.P. 2020. **Management Information Systems: Managing the Digital Firm**. Harlow, UK: Pearson Education.
- [47] Manager Online. 2019. **Somkid thanked Google for Thailand for helping Thai people access technology and proposed to set up a regional office in Thailand**. Retrieved from <https://mgronline.com/cyberbiz/detail/9620000109417> [In Thai]
- [48] Marini, F. (Ed.). 1971. **Toward a New Public Administration: The Minnowbrook Perspective**. Scranton, PA: Chandler.
- [49] Microsoft. 2019. **Thailand's AI-powered healthcare system curbs government costs, helps save lives**. Retrieve from <https://customers.microsoft.com/en-us/story/ministry-of-public-government-health-azure-ai-thailand>
- [50] Microsoft. 2020a. **BAAC harnesses power of Microsoft's world-class cloud platform in mission to help Thai farmers overcome COVID-19 impact**.
- [51] Retrieve from <https://news.microsoft.com/th-th/2020/06/24/baac-agri-en/Microsoft.2020b>. **Microsoft Thailand strengthens partnership with Ministry of**

- [52] **Higher Education elevating online learning with Microsoft Teams for Education – covering 150 universities across country.** Retrieve from <https://news.microsoft.com/th-th/2020/03/26/teamsforedu-en/>
- [53] Microsoft. 2020c. **Microsoft partners with RISE to launch the “Hack the Future: Business Rebound Edition” project to accelerate innovation for Thai SMEs to recover business after the crisis.** Retrieved from <https://news.microsoft.com/th-th/2020/06/18/rise-hackthefuture-th/> [In Thai]
- [54] **Ministry Enhancing Act (Book no.17) 2016 (Establishing the Ministry of Digital Economy and Society).** Retrieved from <http://www.ratchakitcha.soc.go.th/DATA/PDF/2559/A/080/1.PDF> [In Thai]
- [55] **National Security Council Act 2016.** Retrieved from <http://web.krisdika.go.th/data/law/law2/%CA19/%CA19-20-2559-a0001.pdf> [In Thai]
- [56] O’Leary, R.; Van Slyke, D.M.; Kim, S. (Eds.). 2010. **The Future of Public Administration Around the World: The Minnowbrook Perspective.**
- [57] Washington D.C.: Georgetown University Press. OpenDurian. 2017. **About us.** Retrieved from <https://www.opendurian.com/about/> [In Thai]
- [58] Osborne, D. and Gaebler, T. 1992. **Reinventing Government: How the Entrepreneurial Spirit is Transforming the Public Sector.** NY: Addison-Wesley.
- [59] Osborne, S.P. 2003. **The Voluntary and Non-Profit Sector in Japan: The Challenge of Change.** London: Routledge.
- [60] Ostas, D. 2010. Civil Disobedience in a Business Context: Examining the Social Obligation to Obey Inane Laws. **American Business Law Journal** 47 (2): 291 – 312.
- [61] **Personal Data Protection Act 2019.** Retrieved from http://www.ratchakitcha.soc.go.th/DATA/PDF/2562/A/069/T_0052.PDF [In Thai]
- [62] Peters, B. 2001. **The Future of Governing.** Lawrence, KS: University Press of Kansas.
- [63] Privacy International. 2017a. **Privacy International investigation exposes the role of Microsoft in Thailand human rights abuse case.** Retrieved from <https://privacyinternational.org/press-release/683/privacy-international-investigation-exposes-role-microsoft-thailand-human-rights>
- [64] Privacy International. 2017b. **Who's That Knocking At My Door? Understanding Surveillance In Thailand.** Retrieved from https://privacyinternational.org/sites/default/files/2017-10/thailand_2017_0.pdf
- [65] Rawls, J. 1999. **A Theory of Justice.** Cambridge, Massachusetts: The Belknap Press of Harvard University Press.
- [66] Roach, J. 2018. **Under the sea, Microsoft tests a datacenter that’s quick to deploy, could provide internet connectivity for years.** Retrieved from <https://news.microsoft.com/features/under-the-sea-microsoft-tests-a-datacenter-thats-quick-to-deploy-could-provide-internet-connectivity-for-years/>
- [67] **Royal Decree on determination of agencies and businesses that data controllers are not subject to Personal Data Protection Act B.E. 2562 (A.D. 2019) B.E. 2563 (A.D. 2020).** Retrieved from http://www.ratchakitcha.soc.go.th/DATA/PDF/2563/A/037/T_0001.PDF[In Thai]
- [68] Samejaidee, T. 2019. **Microsoft, ministry to develop AI lab.** Retrieve from <https://www.bangkokpost.com/business/1793919/microsoft-ministry-to-develop-ai-lab>

- [70] Shafritz, J.M.; Russell, E.W.; Borick, C.P. 2017. **Introducing Public Administration**. NY: Routledge.
- [71] Siam Blockchain. 2017. **The survey of Thais on the usage of digital coin**. Retrieved from <https://docs.google.com/spreadsheets/d/1C Nulc9lFp5keCYpI-WEuJjicwRieYfxim8oD7pouKGI/edit#gid=0>
- [72] The Nations. 2016. **In meeting with Prajin, Facebook reiterates firm stand on users' privacy**. Retrieved from <https://www.nationthailand.com/national/30300241>
- [73] Thoreau, H.D. 1849. Resistance to Civil Government. In Peabody, E.P., R.W. Emerson, N. Hawthorne (eds.), **Aesthetic Papers**, pp. 189 – 211.
- [74] Boston: The Editor. Toomgum, S. 2019. **Amazon's EdStart helps deliver Thailand's OpenDurian Corporate**. Retrieved from <https://www.nationthailand.com/business/30372231>
- [75] Tortermvasana, K. 2018. **Google vows to 'Leave No Thais Behind'**. Retrieved From <https://www.bangkokpost.com/business/1505830/google-vows-to-leave-no-thais-ehind#:~:text=The%20strategy%20was%20announced%20Thursday,a%20partnership%20with%20CAT%20Telecom>.
- [76] **Treaty of Westphalia**, Holy Roman Emperor and the King of France and their respective Allies, October 24, 1648. Retrieved from <https://is.muni.cz/el/1423/podzim2008/MVZ430/um/Treaty-of-Westphalia.pdf>
- [77] Tor Metrics. 2020a. **Relay users [Thailand]**. Retrieved from <https://metrics.torproject.org/userstats-relay-country.csv?start=2020-04-06&end=2020-07-05&country=th&events=off>
- [78] Tor Metrics. 2020b. **Bridge users by country [Thailand]**. Retrieved from <https://metrics.torproject.org/userstats-bridge-country.csv?start=2020-04-06&end=2020-07-05&country=th>
- [79] United Nations Economic Commission for Europe. 2017. **Innovation in the Public Sector**. NY and Geneva: United Nations.
- [80] Vietnam Investment Review. 2014. **Thai Law Enforcement Agency optimises investigations with Microsoft solutions**. Retrieved from <https://www.vir.com.vn/thai-law-enforcement-agency-optimises-investigations-with-microsoft-solutions-31172.html>
- [81] Walzer, M. 1967. The Obligation to Disobey. **Ethics** 77 (3): 163 – 175.
- [82] Warren, T. 2018. **Microsoft sinks a data center off the Scottish coast**. Retrieved From <https://www.theverge.com/2018/6/6/17433206/microsoft-underwater-data-center-project-natick>
- [83] White, L.D. 1926. **Introduction to the Study of Public Administration**. NY: The Macmillan Company.
- [84] Wichowski, A. 2020. **The Information Trade: How big tech conquers countries, challenges our rights, and transforms our world**. NY: HarperOne.
- [85] Zain, Z.M. and Yusoff, M.A. 2017. Civil Disobedience: Concept and Practice. **Asian Social Science** 13(8): 129- 134.