DIGITAL ECONOMY: A PARADISE OR THREAT IN THE NEW NORM?

LOO-SEE BEH, PhD.
Professor, Faculty of Economics & Administration
University of Malaya, Malaysia.
Email: lucybeh@um.edu.my

Abstract

The digital economy is exponentially expanding into every aspect of our lives and industries with sensors, mobile, cloud and big data. This work-in-progress paper will be discussed in 2 parts. Part One will examine the digital firms, fintechs that leverage their capability and large customer base in the digital financial services that include Grab and GoJek and the associated services of digital wallets in Malaysia and neighbouring countries who are "enablers" in the digital economy or "disrupters" in a conventional economy with the growing pool of tech-savvy consumers and rising tide of digital economy and underpinning consumption.

In Part Two, can the digital economy protect the safety, security and privacy of its customers and citizenry? Herein lies the problem – disruptive digital technology, cyberattacks, compromising data breach committed by hackers and fraudsters that could lead to cybercriminals and associated activities of identity theft and so forth. How does the government keep pace with the rapid change and continuing digital disruption in compliance within the legal requirement as innovation is exponentially experienced? This paper will illustrate the security condition of the digital economy risks and the preparedness in facing them as both business and personal risks in Malaysia and global comparison, wherein possible, including existing policies in reinforcing defense in the new norm.

INTRODUCTION

Digital solutions now permeate all aspects of our daily life, from the ability to make mobile payments, to relying on real-time traffic apps to increase the efficiency of travel. The digital economy is exponentially expanding into our everyday aspects of our lives and industries. Many countries are embracing the booming digital economy for the creation of higher-paying jobs, improvement of productivity, as the new driver of the economy.

The current digital economy embraces the creation and operation of industrial systems with artificial intelligence (AI) elements and global digital infrastructure that allows for the creation of 'smart cities', 'digital currencies', 'hybrid or electric cars' and so forth. As such the following concepts emerged: "Digital Economy" (2001), "Crypto-currency" and "Blockchain" (2008), "Industrial Internet" (2012), "Internet of Things" (2012), "Industry 4.0" (2013), "Second-Machine Age" (2014), and "The Fourth Industrial Revolution" (2016).

The growth of digital technologies, social networks and smartphones has contributed to faster and more targeted customers with creation of new companies and startups. These include Uber, Grab, Amazon, Alibaba, Facebook, Netflix, iTunes, Lyft, etc. which become a paradise, if one may say so but susceptible to innovation are those companies under the threat of substitution by the above new creation, software products or artificial intelligence that see the demise of Kodak, Borders, Blockbuster, etc.

PART ONE

Part One will examine the digital firms, fintechs that leverage their capability and large customer base in the digital financial services that include Grab and GoJek and the associated services of digital wallets in Malaysia and neighbouring countries who are "enablers" in the digital economy or "disrupters" in a conventional economy with the growing pool of tech-savvy consumers and rising tide of digital economy and underpinning consumption.

Today, Southeast Asia has 350 million internet users – a mobile first consumer class larger than the entire population of the US. The number of users in Southeast Asia buying physical goods through e-commerce platforms doubled from less than 50 million in 2015 to over 120 million in 2018. In the same period, active users of ride-hailing services such as GoJek and Grab quadrupled from 8 million to 35 million (The Edge, December 3, 2018). Such modern alternative is seen as a disruptor or a competitor to the conventional taxi services though more as enablers to the consumers. The taxi companies strongly protested the existence of both ride-hailing services in the respective countries as they felt threatened and rivaled by the disruptive innovations. Today, it is viewed with a modification as these conventional taxi drivers could also become Grab or Go-Jek drivers, thus seen as an enabler in the mindset change, that these ride-hailing services are no longer a threat to their economy.

GoJek was founded in 2010 with only 20 drivers but increased to 800 drivers in 2015 primarily with experienced motorcycle riders in Jakarta, Bandung, Bali and Surabaya and has become a market segment in shipping goods, ordering food, shopping and transport in the cities with the development of application-based online transportation.

GrabTaxi Holdings Pte. Ltd. which was founded in 2012 is a Singapore-based technology company that offers ride-hailing, ride sharing, food delivery service and logistics services

through its app in Singapore and neighbouring Southeast Asian nations Malaysia, Indonesia, Philippines, Vietnam, Thailand, Myanmar, and Cambodia.

Southeast Asians are not just passive consumers in the internet economy. They are building leading companies in the ecosystem. Local businesses rule e-commerce, the fastest growing sector in the internet economy. Lazada, Shopee, and Tokopedia account for nearly 70% of the US$23 billion spent on online shopping in 2018. As impressive as current developments, the internet economy currently only accounts for 2.7% of Malaysia's GDP, thus there is a huge opportunity for accelerated growth.

DIGITAL CURRENCIES

Cash is being used less and less with the digital payment systems – PayPal, ApplePay,Venmo in the West; Alipay and We WeChat in China; M-Pesa in Kenya; Paytm in India, SamsungPay, Apple Pay in Southeast Asia that offer attractive alternatives to services once provided by traditional commercial banks. Most of these fintech innovations are still connected to traditional banks and none of them rely on cryptocurrencies or blockchain. Cryptocurrencies like Bitcoin are not actually anonymous given that individuals and organizations using crypto-wallets still leave a digital footprint. Further, authorities that legitimately want to track criminals and terrorists will soon crack down on attempts to create crypto-currencies with complete privacy.

Nevertheless, the fragmentation of national payments solutions with the majority of Southeast Asians still preferring cash also creates friction and transaction costs for all internet economy sectors. An open and interoperable digital payments system and the free flow of data in the region may help consumers and businesses seamlessly transact across borders.

ARTIFICIAL INTELLIGENCE (AI) AND AUTONOMOUS VEHICLES (AVs)

AI's role is already very significant yet still transforming continuously. AI-based equipment is being used to track, police and solve crime while its military applications are already well practiced. The AI market is already huge with its applications in healthcare, elderly care and precision medicine and surgery amongst many others. Much of the AI development and applications are driven by business considerations and thus in turn, shape politics, law, influencing science and technology and how AI and its users are seen and understood.

In Southeast Asia, Singapore is already preparing for the future. In a Jan 31 2019 media conference, its regulators and industry players issued a provisional set of national standards, known as Technical Reference 68 (TR 68), to guide the fast-evolving industry. According to a media statement by Enterprise Singapore, the Land Transport Authority, Standards Development Organisation and Singapore Standards Council, TR 68 will promote the safe deployment of fully driverless vehicles in the city state and could be the first of its kind. It added that the standards are meant to guide the industry in the development and deployment of vehicles in the Society of Automotive Engineers Level 4 and 5 bands – vehicles that are partial and fully autonomous in all driving scenarios (The Edge, February 11, 2019).

Naturally, the road to full autonomy in transport will likely be long and full of obstacles, apart from the forerunners such as Waymo (Google's self-driving project owned by Alphabet), Baidu Inc and Aptiv plc, auto juggernauts such as GM, Daimler, Ford and Audi AG are also racing to introduce their versions of AVs and their potential to transform the automotive industry. Delian is one of the early comers in China by investing in a variety of technologies

that support AVs and the focus has been mostly on Chinese start-ups working to develop sensors, semiconductors, hardware, software and telecommunications system.

THE RISE OF ASEAN FINTECH

Funding into financial technology (fintech) firms have grown in ASEAN-6 (Indonesia, Malaysia, Philippines, Singapore, Thailand and Vietnam) from US$24 million in 2014 to US$458 million in October 2018. Singapore leads with 48.5% contributing US$222 million. (The Edge, November 26, 2018). For fintech firms to grow, they must find opportunities to increase their customer base, connect with partners and investors, and expand into new markets. ASEAN's favorable demographics, an expanding middle class and strong economic growth have attracted an increasing number of fintech firms to set up operations in the region.

Close to half of ASEAN's populations are below 30. As more of the young citizens join the workforce and with rising affluence, consumption in the four key areas – apparel, food, accommodation and transport will continue to increase. Given the rising popularity of digital, internet and mobile technologies, connectivity has since emerged as a new pillar underpinning consumption.

In the mobile payment space, we see that techfin firms who are technology players that leverage their capability and large customer base to enter the financial services industry globally. Examples include Grab and GoJek which have jumped on the digital financial services bandwagon with the launch of their respective digital wallets GrabPay and GoPay, riding on their large customer base.

In the banking industry, there is greater collaboration between banks and fintech firms. Banks are increasingly seeing fintech firms as enablers instead of disrupters with both coming together to engage with ASEAN consumers and corporates in new ways. The breadth of technological innovation ranges from blockchain-based corporate lending to lifestyle-based insurance.

COLLABORATIVE INNOVATION

When Cyberjaya was launched as a smart city in May 2017, the initiatives include the Mimos and Futurise Centre as a hub for corporations, universities, start-ups and entrepreneurs as well as innovation outfits such Microsoft HoloLens and AI Lab and the United Nations Technology Innovation Lab to converge and develop future innovations. Futurise Centre will serve as a nucleus for collaborative innovation, specifically the incubation of new ideas and solutions by local innovators and creators in the development of a futuristic innovation ecosystem geared towards Industrial Revolution 4.0 in Malaysia. Cyberjaya is looking to launch two more co-working spaces – CoCre8 (for companies and startups that want to develop solutions for the creative industries) and CoMedic8 (a centre of excellence for healthcare). The latter is currently being built with Cyberjaya Hospital. Cyberview has also signed a memorandum of understanding with the Pivot City Innovation District in Geelong, Australia. Pivot City had taken over some paper mill buildings and is turning them into a testbed for smart city solutions for Melbourne and Geelong (The Edge, February 11, 2019).

Startup community is also a form of the new norm including the fintechs, etc., which is multifaceted, with global start-up enablers that include privately backed and government-led incubators, accelerators and international venture builders. In Singapore these include Antler, Entrepreneur First and German Accelerator. The agency SGInnovate overseeing start-ups has

also introduced the Global Innovation Alliance in 2017 with a focus on technology and innovation.

Recognizing the value of technology innovation, regulators in Indonesia, Malaysia, Philippines, Singapore and Thailand have introduced regulatory sandboxes. These sandboxes test fintech innovations and encourage fintech firms to innovate faster and at lower costs.

PART TWO
Digital technology has transformed modern life, but it also has been embraced by fraudsters, hackers and social media trolls. Therefore, it is understandable that we have every reason to be concerned about the misuse or abuse of leaked personal data by cybercriminals.

As technologies such as sensors, mobile, cloud and big data become more embedded within industries, a reliable approach to cybersecurity will be required at all levels of a corporation. Business leaders need to understand not just the potential of digital technologies, but also how to effectively protect both their own and customers' data.

AI depends heavily on information especially big data, in order to improve upon human thought processes and behavior. The issue of breach of privacy has received considerable attention as individual freedoms, privacy and property rights have allegedly been violated. Frequent apologies by tech companies for earlier breaches and even the sale of personal data have become so routine despite the enacted laws.

With high profile cyber attacks continuing to dominate the news worldwide, there are prevailing concerns that the exponential growth of the digital economy is being undermined by an erosion of trust in, and growing fear of, digital technology. As such, can we fault the general public for having an apprehensive attitude towards digital technology at particular times e.g. when a massive data breach saw the customer data of more than 46 million mobile subscribers in Malaysia leaked in 2017. This was followed by another reported data breach in early 2018 that saw the personal details of about 220,000 Malaysian organ donors and their next of kin leaked online. Similar data breach occurred in the Singapore healthcare system in 2018, in Pentagon in recent years, etc.

Another most recent threat on February 13, 2019, Malta's largest bank, The Bank of Valletta was the target of a cyber attack with hackers attempting to withdraw 13 million Euro. The bank in which the government is the largest shareholder shut down its systems, closing branches and ATMs and suspending mobile, internet banking and website. Hackers attempted to transfer funds to banks in the Czech Republic, Hong Kong, Britain and the United States. The transactions had been traced and were "being reversed" (The Star, February 15, 2019).

Thus far, how prepared are we in facing the above threats? Policymakers generally lag behind in regulating AI, especially in developing countries. Regulating what is little known or understood remains especially challenging. AI may help us do things better, faster and more efficient, yet we must recognize its multiple functions to begin to understand its complexity. Legislation and industry regulations must keep up with such changes and challenges. What are the responsibilities of businesses creating, selling and using AI? Will the rise and spread of AI lead to new modes of mass surveillance, control and manipulation, even digital dictatorship or authoritarianism? It is much agreeable to say that businesses and government could ensure the optimum development and use of AI for the greater benefits in the face of imperatives of profits and power. But many do worry about how AI is being made use of and the potential for further

abuse yet unclear about how this could impact on government interventions and social collective action.

The biggest bottleneck to IoT adoption would be security, or the lack of it. Many IoT enabled devices lack even basic security as many IoT standards and protocols create security blind spots. The scale and scope of IoT deployments hinder visibility into security incidents as there is a lack of clarity of responsibility regarding privacy and security, according to Forrester Inc. The IoT Cybersecurity Improvement Act of 2017 will use the US government's buying power to signal the basic level of security that IoT devices sold to government agencies need to have. For example, the bill would require the vendors of IoT devices purchased by the federal government to ensure that the devices can be patched when security updates are available. The devices should not use hard-coded (unchangeable) passwords and vendors should ensure that the devices are free from known vulnerabilities when sold (The Edge, February 11, 2019).

We are no doubt at a critical juncture in our use of technology in the digital economy era. It can be used to create further digital disruption as enablers for the benefit of the public or it could become a platform for cybercriminal activity, both serving as a paradise or a threat depending on the receiver end. Legislative and administrative requirements need to be updated to keep pace with the rapid change of technologies and the authorities ensure a common pursuit of interests against cybersecurity breach with new training and updated knowledge. Thus, the role of the government is critical in establishing regulations and able to well-regulate and monitor the disruptive innovations in the perspective of serving as a paradise or a threat in the new norm.

REFERENCES

The Edge (Malaysia), February 11, 2019.

The Edge (Malaysia), December 3, 2018.

The Edge (Malaysia), November 26, 2018.

The Star, (Malaysia), February 15, 2019.