Thailand's Computer Crime Act: Security vs. Freedom of Expression

Danuvasin Charoen*

In the Summer of 2012, two independent decision makers sat in their respective offices on opposite sides of the globe, attempting to determine the best course of action with respect to the Computer Crime Act (hereinafter referred to as "the Act") that the Thai government had promulgated in 2007. The Act had been motivated by the growing concern over computer and Internet crimes, but had met mixed reactions from various interest groups, including domestic and foreign Internet firms and political camps.

On one side of the decision was Mr. Thomas Dungen, chief executive office (CEO) of Fatbook.com, who was trying to decide whether to launch a Thai version of his increasingly popular social website. There was no question in his mind but that the need and market potential existed and that there would be a low breakeven point and a correspondingly high return on investment -- financial outcomes that would benefit the firm tremendously as the day approached when he and his collaborators opted to take the company through an initial public offering (IPO). His uncertainty and hesitation were attributable to his concern that that the Act spread liability for infractions rather broadly. That is, the internet service provider could be -- and in one recent instance, had been -- held jointly liable with those who were *directly* responsible for committing a particular offense under the Act. This provision, Dungen felt, had the potential to

---

* This case study was written by Dr. Danuvasin Charoen, Assistant Professor of Management Information Systems and Technology, Graduate Faculty of Business Administration at the National Institute of Development Administration (Thailand) and is based archival research. NIDA cases are developed solely as the basis for class discussion, and are not intended to serve as endorsements, sources of primary data, or illustrations of effective or ineffective administrative or managerial practice.

cause the company a lot of grief. Were his firm to launch a Thai Fatbook and later learn that an employee or a user stood accused of violating the Act, not only would the firm face a public relations nightmare, but possible suspension of the firm's permission to do business in Thailand, along with the prospect of prison time for whomever the authorities determined to be liable for the violation of the Act.

Dungen found the decision a particularly difficult one to make. On the one hand, the opening of a Thai Fatbook held the always welcome promise of handsome financial gains from additional advertising revenues, along with increased popularity and prestige that would attract even larger numbers of users, thereby yielding a larger base to factor into advertising charges and, in essence, set up a kind of "virtuous cycle." On the other hand, the prospect of later finding himself and his firm accused of having run afoul of certain provisions of the Act due to some website user's actions or inactions and thereby being obliged to defend both his firm and himself personally from criminal prosecution – this was a prospect of unknowable probability that continued to give Dungen great pause. As an entrepreneur of the first order, he appreciated that business gain was always predicated on the taking of a calculated risk. But, he wondered, were the risks in this instance really worth the potential gain?

Meanwhile, at Government House, the seat of the Thai government in Bangkok, Thailand, the Prime Minister, Yingluck Shinawatra, was wrestling with an equally difficult decision — i.e., whether to put her government squarely in favor of rescinding the Act (as some stakeholders were demanding) or in favor of leaving the Act as it was (as other stakeholders were insisting). In common with Dungen, who was wrestling with a different but interrelated facet of the issue in his office half way across the globe, the prime minister was finding that the decision as to which way to go was no easy task, not the least because there were powerful and influential forces on both sides of the issue.

Arrayed in opposition to the law was an amalgam of interests that were convinced that the Act was a serious affront and impediment to freedom of expression and other values deemed essential to the nurturance and preservation of a democratic society. Further, certain political voices within the anti-Act camp were convinced that some provisions of the Act lent themselves to abuse in that they were subject to being used as weapons against upstart political forces that the traditional power centers perceived as threats. These groups were steadfast in the belief that for Thai democracy to take root and flourish, it was of paramount importance that the right of the people to express their views on all manner of issues not be squelched through laws threatening severe retribution.

In addition, among other sub-groups were foreign business interests such as Fatbook who, although not directly engaged in attempts to influence government policy on the matter, were nonetheless accustomed to doing business in environments with less draconian laws governing the uses of advanced communication technology, such as the Internet. These groups not only represented potential new foreign investment, but also avenues by which Thailand's stature as a "technology-ready" society, making maximum use of advanced communication technology, could be enhanced.

Other influential and powerful interest groups, however, had taken a decidedly different position on the Act. For example, the all-important military establishment and their allies in the royalist camp were adamant in their position that the Act was not to be touched. For a variety of reasons, they deemed the law – in particular, its lese majeste provisions -- an important means by which to preserve the essential underpinnings of the Thai state and society. Because of the military's well-known past tendency to employ extra-political means to enforce its views, Prime Minister Shinawatra knew that, quite likely, military personages would be carefully monitoring any actions that she might take concerning the disposition of the Act. Indeed, if she needed any reminder of how decisively the military could act when it felt that a government was proceeding in the wrong direction, the military's dissolution of the government of her elder brother (Thaksin Shinawatra) in September 2006 was a poignant and ever-present reminder.

Keywords: Computer Crimes, IT Security, Computer Crime Act, Freedom of Expression on Internet

พรบ.ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์: ความมั่นคงกับเสรีภาพในการแสดงความคิดเห็น

ดนุวศิน เจริญ*

บทคัดย่อ

ในฤดูร้อนปี พ.ศ. 2555 มีผู้ต้องตัดสินใจสองคนในเรื่องที่เกี่ยวข้องกับ พรบ.ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 อยู่สองคนคือ นายโทมัส ดันแกน ประธานผู้บริหารบริษัท Fatbook ซึ่งคือบริษัทที่ให้บริการในด้านสังคมออนไลน์ที่ใหญ่ที่สุดในโลก และอีกคนคือ นางสาวยิ่งลักษณ์ ชินวัตร นายกรัฐมนตรีหญิงคนแรกของประเทศไทย พรบ.ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ถือว่าเป็นหนึ่งในกฎหมายที่มีการถกเถียงมากที่สุด กฎหมายนี้ถือว่าเป็นกฎหมายแรกของประเทศไทยที่เข้ามาบังคับใช้ในการป้องกันปราบปรามอาชญากรรมที่เกี่ยวข้องกับคอมพิวเตอร์และอินเทอร์เน็ต แต่อย่างไรก็ตาม กฎหมายนี้ก็มีผู้โต้แย้งว่าเป็นกฎหมายที่ลิดรอนสิทธิเสรีภาพในการแสดงความคิดเห็น

สำหรับนายโทมัส ดันแกน กำลังพิจารณาว่าบริษัทควรขยายธุรกิจของ Fatbook มายังประเทศไทยหรือไม่ Fatbook ในประเทศไทยได้รับความนิยมเป็นอย่างมาก มากกว่า 80 เปอร์เซ็นต์ของผู้ใช้อินเทอร์เน็ตในประเทศไทยล้วนเป็นผู้ใช้ Fatbook นอกจากนี้ แนวโน้มของการใช้สังคมออนไลน์มีการเติบโตที่สูงมาก ดังนั้น ตลาดในประเทศไทยถือว่าเป็นตลาดที่น่าดึงดูดมากของ Fatbook สามารถสร้างผลกำไรจากการโฆษณาและการขายสินค้าออนไลน์ รวมทั้งสร้างฐานผู้ใช้จำนวนมากให้กับบริษัทได้ แต่อย่างไรก็ตาม นายโทมัสฯ มีความกังวลเกี่ยวกับกฎหมายในประเทศไทยที่อาจ

---

* กรณีศึกษานี้พัฒนาโดย ผู้ช่วยศาสตราจารย์ พ.ต.ต.ดร. ดนุวศิน เจริญ อาจารย์ประจำสาขาการบริหารระบบเทคโนโลยีสารสนเทศ คณะบริหารธุรกิจ สถาบันบัณฑิตพัฒนบริหารศาสตร์ กรณีศึกษานี้รวบรวมข้อมูลจากแหล่งข้อมูลทุติยภูมิต่าง ๆ โดยกรณีศึกษานี้สามารถใช้ประกอบการสอนวิชาบริหารระบบเทคโนโลยีสารสนเทศ การบริหารความปลอดภัยและความเสี่ยงในระบบเทคโนโลยีสารสนเทศ รวมถึงวิชากฎหมายที่เกี่ยวข้องกับการใช้คอมพิวเตอร์และอินเทอร์เน็ต ลิขสิทธิ์ของกรณีศึกษานี้เป็นของสถาบันบัณฑิตพัฒนบริหารศาสตร์ และผู้ช่วยศาสตราจารย์ พ.ต.ต.ดร. ดนุวศิน เจริญ

สำหรับท่านที่ต้องการสั่งซื้อกรณีศึกษานี้สามารถติดต่อได้ที่เบอร์ 0 2727 3188 หรือเข้าไปที่ www.nida.ac.th หรือ e-mail มาที่ danuvasin@gmail.com

เป็นอุปสรรคต่อความสำเร็จของธุรกิจ เนื่องจาก พรบ.ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 มีข้อบังคับและบทลงโทษที่ค่อนข้างรุนแรงสำหรับการแสดงความคิดเห็นที่ไม่เหมาะสมบนอินเทอร์เน็ต Fatbook เป็นผู้ให้บริการสังคมออนไลน์ไม่สามารถควบคุมผู้ใช้ในการแสดงความคิดเห็นต่าง ๆ ได้ นอกจากนี้ บริษัทก็ยังมีความเสี่ยงทางกฎหมายในกรณีที่ผู้ใช้กระทำความผิดผ่านทาง Fatbook เพราะกฎหมายบังคับให้ผู้ประกอบการต้องมีส่วนในการรับผิดและรับโทษด้วย นายโทมัสฯ กำลังครุ่นคิดว่าผลกำไรที่จะเกิดขึ้นในประเทศไทยจะคุ้มค่าต่อความเสี่ยงทางกฎหมายที่อาจเกิดขึ้นได้

ในขณะเดียวกัน ผู้ที่ต้องตัดสินใจอีกคนคือ นางสาวยิ่งลักษณ์ ชินวัตร นายกรัฐมนตรีหญิงคนแรก ที่ต้องตัดสินใจว่าควรจะมีการแก้ไข พรบ.ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 หรือไม่ การตัดสินใจนี้ไม่ง่ายเลย เนื่องจากในรัฐบาลเองก็มีความเห็นแบ่งเป็นสองฝั่ง ฝั่งหนึ่งมองว่ากฎหมายนี้เป็นเครื่องมือหลักในการบังคับใช้กฎหมายที่เกี่ยวข้องกับอาชญากรรมคอมพิวเตอร์ นอกจากนี้ กฎหมายนี้ยังใช้คุ้มครองความมั่นคงของรัฐ และสถาบันหลักของประเทศ รวมถึง สถาบันศาสนาและพระมหากษัตริย์ สำหรับอีกฝั่งหนึ่งมองว่ากฎหมายนี้ทำให้ประเทศมีภาพลักษณ์ที่ไม่ดีในสายตาของต่างชาติ โดยเฉพาะอย่างยิ่งองค์กรที่เกี่ยวข้องกับสิทธิมนุษยชนมองว่ากฎหมายนี้ลิดรอนสิทธิพื้นฐานของมนุษย์ คือสิทธิในการแสดงความคิดเห็นอย่างเสรีภาพ

นอกจากนี้ บริษัทต่างชาติอื่น ๆ ก็ไม่มีความมั่นใจในการลงทุนธุรกิจที่เกี่ยวข้องกับอินเทอร์เน็ตในประเทศไทย ซึ่งรัฐบาลได้ประกาศจุดยืนของประเทศตลอดมาว่าประเทศไทยจะเป็นผู้นำในการใช้เทคโนโลยีที่ทันสมัย พร้อมกับดึงดูดการลงทุนในด้านเทคโนโลยีสารสนเทศและการสื่อสาร ซึ่งสิ่งเหล่านี้ล้วนมีความจำเป็นต่อการสร้างความสามารถการแข่งขันของประเทศทั้งสิ้น ในทางกลับกันประชาชนหลายกลุ่มในประเทศ ไม่ต้องการให้มีการเปลี่ยนแปลงใด ๆ ในกฎหมาย หรือถ้ามีการเปลี่ยนแปลงก็ต้องการให้บทลงโทษมีความเข้มข้นขึ้นโดยเฉพาะอย่างยิ่งมาตราที่เกี่ยวข้องกับการหมิ่นพระบรมเดชานุภาพ ซึ่งถือว่าเป็นภัยต่อความมั่นคงของประเทศ

ณ ตอนนี้ นายกรัฐมนตรีหญิงคนแรกของประเทศไทย รู้สึกเหมือนตกที่นั่งลำบาก เนื่องจากเธอรู้ว่าถ้ามีการเปลี่ยนแปลงกฎหมายนี้ อาจนำไปสู่การเป็นประเด็น หรือข้ออ้างในการปฏิวัติรัฐประหาร เพราะพี่ชายของเธอคือ พ.ต.ท.ทักษิณ ชินวัตร เองก็เคยถูกรัฐประหารเนื่องจากถูกมองว่าไม่มีความจงรักภักดีต่อสถาบันพระมหากษัตริย์ แต่ในทางกลับกันถ้าเธอไม่เปลี่ยนแปลงกฎหมาย ประเทศอาจเสียโอกาสในการดึงดูดการลงทุนจากบริษัทต่างชาติ รวมถึงสร้างความสามารถการแข่งขันของประเทศผ่านทางเทคโนโลยีที่ทันสมัยได้

คำสำคัญ: อาชญากรรมคอมพิวเตอร์ กฎหมายคอมพิวเตอร์ การกระทำผิดเกี่ยวกับคอมพิวเตอร์ เสรีภาพในการแสดงความคิดเห็น

Overview of Thailand

Located in the strategic centre of the South-East Asian peninsula and bordered by the Gulf of Thailand, Myanmar, Laos, Cambodia, and Malaysia, the Kingdom of Thailand was the world's 50th largest nation in land mass (513,115 square kilometers, or 198,120 sq mi) and the 20th largest country in population (estimated in 2010 as slightly more than 67 million people). The country was divided into six regions (North, Northeast, East, South, West, and Central) plus the administrative region comprising the capital, Bangkok ("*Krung Thep*"), which was by far the most significant urban area in the country.

Demographically, the country was comprised of a majority of ethnic Thais, but also had a substantial population of persons of Chinese descent (14%), as well as a scattering of other distinct ethnic groups (e.g., the peoples of the several so-called "Hill Tribes"). Approximately 71% of the population fell into the 15-64 age group, although a significant portion (nearly 20%) were in the 0-14 age group and slightly more than 9% were in the 65 years and older group. A 50:50 ratio of males to females pertained in each age group. The population growth was 0.566% as of 2011, which represented a decline from the previous year. Culturally, the country had been shaped by many influences, including the ancient civilizations of India, China, and Cambodia. However, Buddhism -- the state religion, as well as the religious preference of nearly 95% of the population -- had exerted the most profound influence on the ethos and mores of Thai society. The country was also alone among its Southeast Asia neighbors in the distinction of never having been a colony at any point in its nearly 1,000-year history.

The country enjoyed a high level of literacy, with nearly 93% of the population who were 15 years old and over able to read and write. Education was provided mainly by the Thai government through the Ministry of Education and was free through the twelve years of school, but was compulsory only through the first nine years.

In 1932, the absolute monarchy that had prevailed for seven centuries was replaced by constitutional monarchy, with a prime minister as the head of government and a hereditary monarch as the head of state. Despite the introduction of the constitutional monarchy system of government, Thai people continued to respect and revere the King much as they did during the period of absolute monarchy. As reflected in the tri-colored national flag, the king (represented by the blue middle bar) was one of three symbols of Thailand together with the nation (represented by the two red outer bars) and religion (represented by the two white bars abutting the blue).

In concert with the traditional structure of parliamentary systems of governance, the Thai executive branch was also an active participant in the legislative branch of government. An independent judiciary with a supreme court of final authority comprised the third branch. Since the reformation, Thailand had undergone 18 military coups d'etat and 17 constitutions and charters, reflecting a high degree of political instability. Moreover, throughout the reform period, Thailand had experienced many political crises, such as Black May in 1992 and the recent Yellow Shirt and Red Shirt protests, which again demonstrated the pronounced fragility and instability of the Thai polity.

The electoral victory of the Pheu Thai Party in the 2011 elections not only brought to the premiership the first female prime minister, but also the first head of government with extensive experience in the information and communication industry. Khun Yingluck had earlier served as president of the Advanced Information Service, a major Internet service provider founded by her elder brother, deposed Prime Minister Thaksin Shinawatra. Not only had her party campaigned on a pledge of free public WiFi, broadband Internet, and One Tablet (computer) per Child, the new Prime Minister had widely broadcast her vision and determination to make information and communication technology (ICT) the basis for Thailand's competitiveness going forward. Attracting IT investment from the world class companies was to be a core enabling strategy for the achievement of the new plateau of competitiveness. In this connection, she was aware of the possibility – however fraught with potential peril -- that some laws and regulations might need to be either "tweaked" or altogether amended to create an attractive investment context.

Information and Communication Technology in Thailand

The information and communication technology (ICT) business was comprised of four main segments: computer hardware, computer software, computer services, and telecommunication (wired and wireless). Driven by the increasing use of technology in all aspects of society, the industry had been growing rapidly in Thailand as in other countries around the globe, as an ever-expanding diversity of products, lower prices, and wider access to knowledge about how to utilize the various technologies bolstered demand in the public, private, and civil society sectors. In consequence, by 2010, the Thai ICT market, accounting for 11% of the GDP, had risen to become one of the largest in the Southeast Asian region and was projected to grow at a compound annual growth rate of 12% over the 2010-2014 period [1]. The total value of Thai domestic spending on IT products and services, which had been in the vicinity of US$5.4bn in 2010, was expected to reach US$8.7bn by 2014 [1].

Increased usage of the Internet and software applications [2] had steadily pushed upward the overall market value of the industry. Total ICT market value increased every year from 2009 to 2011, when it reached a value of $22,621 million, with a solid 11.7% growth from the previous year. By far the largest contributor to the market value was the telecommunications industry, which accounted for 61.7% (or $13,945 million) of the total ICT market. The remaining segments, in declining order of the magnitude of contributions to the overall market value, were computer hardware shares (at 14.8%, for a market value of $3,350 million), software shares (at 12.4%, for a market worth of $2,807 million), and services (at 11.1% shares, for a market value of $2,519 million) [1-2].

Underlying the above-cited market values and growth rates of the several industry segments lay distinct behaviors concerning the use of ICT technology. For example, on the institutional side, while every business trade and service had been able to increase its efficiency in lowering production costs and creating new markets for products and services, the hospital business in Thailand was the one in which the proportion of employees using computers and the Internet at work was the highest (100% and 90%, respectively), as shown in Appendix 1. The next highest in utilization were manufacturing, travel agencies, construction, and business trade and services, respectively.

However, small and medium enterprises (SMEs) had been slow to adopt ICT, despite the fact that research had indicated the positive effect of ICT on firm performance in terms of creating productivity, profitability, market value, and market share. Further, the size of the particular establishment impacted the usage of ICT. As shown in Appendix 1, establishments with fewer than 16 persons used ICT to a slight degree: computer usage -21.9%; Internet usage -14.2%; and websites -6.2%. By contrast, establishments with 16 persons or more used ICT at a high proportion, e.g., with more than 81.1% of establishments using computers [3].

Among educational institutions, 99.7% of primary educational institutions had computers, while other levels of educational institutions had computers in every institution. Further, the overwhelming majority of educational institutions had Internet access. For instance, as can be seen in Appendix 1, Internet access for primary educational institutions, at the vocational and non-formal education levels, and in the higher education institutions, was 97.2%, 99.0%, and 100.0%, respectively.

While the proportion of the population using computers and the Internet (29.3% and 20.1%, respectively, as of 2009) had increased less robustly than the proportion using mobile phones (56.8%), Thailand nevertheless was ranked 9th in Asia in terms of Internet users in 2011

(see Appendix 2) [4]. Moreover, the Internet access of households had continued to increase, albeit rather modestly, from 5.7% in 2004 to 9.5% in 2009; and, broadband Internet access had increased from 52.8% in 2006 to 55.1, while fixed-line telephones decreased from 23.4% in 2004 to 21.4% in 2009 [3].

In 2012, Thailand was ranked 39th (out of 142 countries) in the global competitiveness report conducted by the World Economic Forum. It also was ranked well below the world average on all of the factors related to technology, despite the fact that information technology and telecommunications had been a major factor driving the competitiveness of certain sectors of the country. More specifically, the major problems for Thailand were concerned with the "pillar of technological readiness" – a measure used by the World Economic Forum to assess a nation's capacity to utilize information and communication technologies. Thailand was ranked 93th in number of Internet users, 82th in availability of the latest technologies, 75th in firm-level technological absorption, 77th in broadband Internet subscriptions, and 83th in Internet bandwidth [4]. The vision of an ICT-driven Thailand suggested that any and all impediments to improvement on these measures be accorded focused attention and action.

No one could deny that over the past twenty years, the Internet had transformed many aspects of modern life in Thailand. People could communicate and collaborate faster and better due to the Internet, and the Internet has become a necessary tool for both business and for leisure. As of June 2011, there were 18 million people (accounting for 27% of the population) accessing the Internet [5]. However, the emergence of the Internet had not brought unalloyed benefits. Rather, like many new technologies at their birth and early stages, the Internet brought a new set of issues and challenges. More specifically, one of the fastest-growing crimes in Thailand, as in a number of other countries around the world, was crime related to the use of computers and the Internet [6], and these crimes could have a negative impact on both businesses and individuals.

National Responses to Cyber Crime

As evidence had mounted that computer and Internet crime could seriously threaten ICT infrastructure, commercial interests, and public policies, more individual nation-states had responded with the development of legal codes to combat computer-related crimes [7]. Because these codes tended to reflect the nature of cyber crimes that had emerged to date in individual countries, there were differences among countries with respect to what types of computer and Internet crimes were covered. (See Appendix 3.) Thus, some cyber crime infractions were included in some national

legal codes but not in others. However, as shown in Appendix 3, among those countries that had promulgated laws against computer and Internet crimes, most addressed some or all of the following specific infractions:

1. unauthorized access;
2. illicit tampering with files or data (such as unauthorized copying, modification, or destruction);
3. computer or network sabotage (via, for example, viruses, worms, Trojan horses, and denial of service attacks);
4. use of information systems to commit or advance "traditional" crimes (such as fraud, forgery, money laundering, and acts of terrorism);
5. computer-mediated espionage;
6. violations against privacy in the acquisition or use of personal data; and,
7. theft of, or damage to computer hardware or software [7].

As shown in Appendix 4, the categories of computer and network misuse that were considered as crimes in Asia showed both convergence and divergence from those in other regions. In general, however, the following infractions were treated as crimes in most Asian countries:

1. theft of electronic data;
2. destruction of, or damage to, a computer system;
3. disclosure of secrets;
4. computer fraud;
5. unauthorized access; forgery of e-documents;
6. defamation;
7. business disparagement; and,
8. obscenity [7].

Each country had different definitions or interpretations of criminal computer acts. For example, the Taiwanese computer crime acts made it an offense to commit fraud by means of the "input [of] false information or commands into a computer or related device, to infringe on copyright, or to appropriate the possessions of others." However, in other countries, fraud was defined as any action of untruthfulness or deception perform through the use of the Internet, or targeted at the technologies that support the Internet[8]. Other countries' actionable infractions included "libel", "business disparagement", "obscenity" ,"making threats", "gambling on the Internet", and "disclosure of secrets" [7]. In some countries, such as Japan and Thai land, unauthorized access to a computer in which people may view secret information were illegal even if there is no damage done to the systems. In Singapore, "unauthorized access", "disclosure of secrets", "destruction or damage of computer systems or electronic data", and "computer fraud" were illegal. In Malaysia, the illegal acts included defamation and libel,

business disparagement, and obscenity offenses. In Hong Kong, the illegal acts included "defamation", "business disparagement", "offenses against e-mail", "damage and destruction", "computer fraud", and "theft of electronic data". In China, where computer crimes were included in Articles 285-287 of the Criminal Code, the offenses included "illegally interfering in the operation of a computer system," which is punishable by a minimum sentence of five years in prison [7]. In Vietnam, under article 88 of the penal code pertaining to "conducting propaganda against the Socialist Republic of Vietnam", it was illegal to post any information that criticized the government or the ruling Communist party [9-10].

The Case of Thailand: Cyber Crimes and the Vision of an ICT-Infused Society

A major reason why Internet and computer criminality had become a sufficiently visible and serious a phenomenon as to precipitate the Thai Computer Crime Act had to do with the country's long-term plans for utilizing the advantages of ICT technology as the linchpin of the strategy to develop the country. Pursuant to this vision, the government's "FRAMEWORK 2010" plan encapsulated the goal of developing the country into a "Wisdom and Learning Society" in which E-industry, E-commerce, E-government, E-education, and E-society – all enabled and propelled by the latest advancements in information and communication technology -- were to play a prominent role. Cyber crime, an on-going and growing problem in Thailand, was considered a serious threat and potential danger because, left unchecked, it could easily interfere with, corrupt, and defeat desired outcomes in each of the "E-sectors" that had been targeted by the government.

As can be seen in the chart below, technology crime cases had surged dramatically between 2010 and the first ten months of 2011. According to the Technology Crime Suppression Division of

Thailand, computer crime offences totalled 73 cases in 2010, but then virtually exploded to 431 cases during *just the first ten months of* 2011 – a nearly five-fold increase. *Content*-related offences by themselves (e.g., importation of forged or false data; possession or distribution of pornographic materials, use of computer data in such a manner as to threaten or compromise Kingdom security) had skyrocketed by a factor of more than 17.5 times (i.e., from 21 in 2010, to 387 in 2011). The most prevalent crimes included attacks against computer data and systems, *lese majeste*, identity theft, defamation, importing a forged or false computer system, Internet gambling, and Internet fraud [11].

Table 1: Technology Crime Case 2010-2011(Jan-Oct)

Nature of Case	2010	2011 (Jan – Oct)
1. System-Related Offences (Illegal access/attacking a system/damaging, destroying, changing the data in computer systems)	16	13
2. Defamation/*lese majeste*	3	6
3. Internet Fraud/Cheating	11	8
4. Internet Gambling	15	14
5. Content-Related Offences (Importation of forged or false data/ Pornographic/Computer data against Kingdom security)	**21**	**387**
5. Others (Extortion, Illegal Drugs)	7	3
Total	**73**	**431**

Apichanont, A. (2011). *Country Report.* Bangkok, Thailand: Technology Crime Suppression Division.

Computer Crime Act of 2007

It had been five years since the post-coup government led by General Surayudh Chulanont had enacted the Computer Crime Act ("Act") that had now become highly controversial, with defenders and detractors particularly unable to find common ground concerning whether the *lese majeste* section should be revised or altogether scrapped. The law's enactment in 2007 coincided with the advent of widespread availability and usage of Internet services among Thai people. As was true in many other countries around the globe, Thais had quickly become avid Internet users, finding it a convenient way to share information among both individuals and businesses. As well, Thai users especially liked the availability of various social media and social networks that provided a new outlet for expressing their opinions and sharing information with others in the network. Web boards, blogs, and social networks enabled people to put their views on various matters (whether socials, economic, political, or other) before others – without being screened or censored, as users could remain anonymous if they so desired. Thus, as computer access and usage mushroomed, so had the popularity of social networks such as Facebook, Hi5, Myspace, LinkedIn and Twitter, each of which had a devoted membership base among Thai Internet users.

Before the enactment of the Act, Thai authorities did not have any specific legal tool with which to address issues such as hacking, disclosure of access passwords to a third party, eavesdropping on computer data, pornography and other "harmful" Internet content, or the liability of ISPs with respect to the content that their "customers" might communicate via their Internet services. Some of these offences could be, and occasionally were, prosecuted under Thailand's Penal Code or the Criminal Code, but the new Act established more specific charges and, in some instances, heavier penalties. Importantly, the Act also gave the competent official some censorship power in form of authority to restrict the dissemination of computer data and to block or shut down websites that the State deemed harmful [10].

The specific crimes addressed by this law ranged across a wide expanse of forbidden acts -- from spreading viruses to "spamming," to an extent that interfered with another's use of a computer, to dissemination of pornographic material, to posting defamatory content, to posting inappropriate contents such as those considered harmful to national security or *lèse majesté,* and beyond. Particularly noteworthy (and troubling to Internet personages such as Fatbook's CEO) was that liability for certain infractions (such as lese majeste) had been broadened to include the ISP and website administrators that hosted inappropriate content (Section 15). In addition, section 14(4) specified a penalty for anyone who helped disseminate inappropriate content, with the act of dissemination including email forwarding, re-tweeting a twitter, or sharing content on Facebook. See Appendix 5 for a listing of the laws addressing computer crime in Thailand.

The Computer Crime Act consisted of two parts. The first part (Sections 8 to 17) covered computer-related offences, and the second part (Sections 18 to 30) covered the roles of authorities and the responsibilities of service providers. In the table below is presented a brief summary of the main provisions of the first section of the Act. (See Appendixs 5 and 6 for a summary of the main provisions of each law concerning computer crime in Thailand.

Main Provisions of the Computer Crimes Act of 2007: Sections 5-16

Section of the Act: Crime	Penalty Provisions
Sections 5 and 6: **Unauthorized Access to a Computer**	Section 5 Penalty: Imprisonment for Up to 6 months and/or fine of up to 10,000 baht (approximately US$300) for unauthorized accessing a computer system Section 6 Penalty: Double the maximum jail term and the maximum fine for disclosing an access code for a computer system in a manner that is likely to cause damage to other people
Sections 7 and 8: **Unauthorized Access to Computer Data**	Section 7 Penalty: Imprisonment up to two years and/or a fine of up to 40,000 baht (approximately US$12,000) for unauthorized accessing computer data Section 8 Penalty: Maximum imprisonment of three years and/or a maximum fine of 60,000 baht (approximately US$1,800) for illegally eavesdropping by electronic means on computer data not intended for use by the general public.
Sections 9 and 10: **Illegal Damage to Computer Data or Computer Systems**	Section 9 Penalty: Imprisonment up to five years and/or fine of 100,000 baht (approximately US$3,000) for illegally damaging, destroying, amending, alerting or adding to a third party's computer data Section 10 Penalty: Provides for the same penalty for illegally suspending, delaying, hindering or disrupting the working of a third party's computer system to the extent that it fails to function as usual.
Section 11: **Spam**	Section 11 Penalty: A fine of up to 100,000 baht (approximately US$3,000), but no imprisonment. **Note:** Spam included sending computer data or emails to another person by concealing or forging the source of the data or email in manner that interferes with the use of that computer by other people.
Section 12: **Causing Damage to Public or National Security**	Section 12 Penalty: Imprisonment up to 10 years and a fine up to 200,000 baht (approximately US$6,000) for sections 9 and 10 offenses where they cause instant or subsequent damage to the public. The penalty can be raised to imprisonment of up to 15 years and a fine of up to 300,000 baht (approximately US$9,000) where the offences are likely to cause damage to computer data or computer systems related to public and national security, economic security, and public service and infrastructure. The maximum imprisonment can be raised to 20 years if the offences cause death.

Section of the Act: Crime	Penalty Provisions
Section 13: **Distributing Computer Programs for the Purpose of Committing an Offence under Sections 5 to 11**	Section 13 Penalty: Imprisonment of up to one year and/or a fine of up to 20,000 baht (approximately US$600) for those selling or disseminating any computer program or set of instructions in order to commit crimes under Section 5 to 11.
Section 14: **Importing Illegal Data into a Computer System**	Section 14 Penalty: Imprisonment of up to five years and/or a fine of up to 100,000 baht (approximately US$3,000) for a variety of offences, including importing false data into a computer system that is likely to cause damage to a third party or the public (sub-section 1), or that can cause public panic (sub-section 2); data constituting an offence against national security (and royal family) under the Penal Code (sub-section 3); pornographic data (sub-section 4), or disseminating these contents.
Section 15: **Role of Internet Service Providers**	Section 15 Penalty: Allows authorities to charge any Internet Service Providers (ISPs) that intentionally supports or gives consent to the commission of an offence under Section 14. The term "intentionally" protects ISPs that are not aware of the contents on their systems. Nevertheless, after the ISPs are informed about the illegal content, this defense no longer applies. If any ISP is found guilty, he or she can face a penalty equal to that imposed on the offender.
Section 16: **Defamation (by visual means)**	Section 16 Penalty: Imprisonment up to three years and/or a fine of up to 60,000 baht (approximately US$ 1,800). This section punishes those who make publicly accessible via a computer system a picture of a third party in a manner that is likely to damage that third party's reputation or to cause that third party to be disgusted or embarrassed.

Source: Computer Crime Act of 2007

Controversies surrounding the Computer Crime Act

As might have been expected, specific sections of the Computer Crime Act had encountered criticism and complaints from various interested parties. Depending on the specific section, these interested parties tended to vary in composition, with certain issues having more salience for, and impact on, some parties than on others. This opposition to nearly all sections of the Act by one interested party or another, or by a shifting coalition of groups, greatly complicated the Prime Minister's decision as to whether to support amendment or rescission of the law.

Too Much Power in the Hands of Governmental Authorities

A major criticism common to a number of objections to specific sections of the Computer Crime Act concerned the scope of authority granted to public authorities. (See Appendix 6 for a summary of the sections of the Act that set forth the roles of the authorities and the responsibilities of service providers, i.e., Sections 18 through 30.) The Act granted authorities vast power to investigate, gather, and confiscate evidence of any suspected computer crimes. For example, Section 18 allowed authorities to copy computer data and/or computer traffic data (log files) from any computer system that was even *suspected* of being used to commit crimes. Under Section 18, the authorities also had legal power to access any computer system and/or computer data, and to seize or attach any computer systems, for up to 90 days, for the purposes of investigation and gathering evidence. Section 20 allows authorities, with the approval of the Minister of Information and Communication Technology, to seek a court warrant limiting the dissemination of information directly or asking an ISP to do so.

To date, the competent authorities had not been shy in using these powers. The *Wall Street Journal* reported that Thai authorities had blocked at least 40,000 web pages in 2010, according to the Ministry of Information and Communication Technology, which was empowered to monitor the Internet in Thailand. However, free speech advocates, dismissing the Ministry's statistic as woefully understated, averred that authorities had actually blocked *at least* 110,000 sites based on government disclosures and their own online checking [12]. Many of the blocked websites contained content deemed to be critical of the government or attacks on Thailand's revered monarchy [12]. Free speech activists argued that the government had intentionally overstated the magnitude and frequency of such threats as a justification to block websites [12] that they felt were too critical of government policies or actions. The most-cited example was the website, www.prachathai.com, an independent news source that contained articles and reports questioning the policies of the government [12]. After nearly

six years of publishing biting comments concerning various government policies and operations, the website was blocked in April 2010, but eventually permitted to resume operation in October 2011.

No Differentiation between Pornographic Content and Artistic Expression

Pornography on the Internet had long been controversial in many countries. While there were few, if any, countries that permitted wholesale posting of such material on the Internet with no restrictions whatsoever, many countries permitted Internet pornography for consenting adults (usually defined as at least 18 years of age) and prohibited the online posting of sexual content only in the case of minors. Further, in recognition of the fact the line between *pornographic* and *artistic* was often blurred, in many countries, particularly the Western liberal democracies, the applicable laws had attempted to make a distinction between "sexual content with no redeeming artistic or social value," i.e., pornography (which was often declared illegal), and artistic expression (which enjoyed a protected status under various types of anti-obscenity laws).

However, Thai law as promulgated in the Computer Crimes Act made no such distinction, which effectively meant that government censors were free to deny that any such distinction could made and thereby subject content in contravention of the Act to the penalties cited in the law itself. Section 14 (3) of the Act stipulated that importing pornographic data into computer systems or Internet could subject the offender to up to five years of imprisonment or a fine of up to 200,000 baht.

This again grated against the beliefs of some critics of the Act. They averred that not only did the Act severely limit the space for legitimate artistic expression, but it also essentially placed the burden on the creator to *prove* that content deemed by the competent authority as "pornographic" was in fact "artistic expression." Such a burden of proof was an almost impossible feat if the competent authority's definition of "artistic" was especially confining -- e.g., limited to landscapes, seascapes, fully clothed people, abstract images, and the like. In other words, the critic complained, "pornography," like beauty, could be said to be *in the eye of the beholder*. The problem was that the "eye" with the final word with respect to prosecution under the Act was that of the competent authority.

Defamation via Computer, with Penalties Greater than those in the Penal Code

Section 16 made it a crime to make publicly accessible via a computer system a picture of a third party in a manner that was likely to "impair that

third party's reputation or cause that third party to be embarrassed." Section 16 only dealt with defamation by *visual* means. It did not cover defamation by means of written text, which was already covered by the defamation provisions in the Penal Code. However, the jail term provided for offenses under Section 16 (i.e., three years years) was higher than that in the Penal Code, which had only a two-year sentence. This contrasted with the crime of *lese majeste* (to be discussed below), for which the penalties in the Penal Code were much higher than those provided for the same offense under the Computer Crime Act.

In most developed, democratic nations, defamation via the Internet applied only to defamatory *statements* on the Internet because of the pronounced subjectivity of the interpretation of images. In addition, the critics had pointed out, criminal defamation – particularly when leveled as a charge pursuant to the online posting of an image of a person -- could be viewed as an inappropriate and unwarranted restriction on freedom of expression [13]. The fact that several website operators and web administrators had been charged with defamation under the Computer Crime Act was very concerning to those opposed to the Act.

Enforcement of Lese Majeste Laws: Maintaining Respect for the Monarchy

Despite having been promulgated to prevent computer and Internet crimes such as hacking computer systems, the Computer Crime Act had yielded mainly prosecutions for online content that allegedly jeopardized *national security*, which included insulting the monarchy [14]. Indeed, due to the domestic political situation since the 2006 military coup that ousted the government of the current Prime Minister's elder brother, Thaksin Shinawatra, *lese majeste* had been the single most prosecuted offence against Internet users and ISPs – and thereby the most controversial issue concerning the Act.

The penalties could be substantial. Under the Act, people convicted of *lese majeste* could be sentenced to between three and five years in prison. (Under the Penal Code, insulting the King was punishable by up to 15 years in prison.) The Act also enabled prosecutors to seek longer sentences if the offenders were found guilty of using the computer and Internet to commit a crime.

In part because of the presumed "chilling effect" of the Act on citizens' right to express themselves freely and in part because of what some considered the "harshness" of the penalties imposed under the Act, Thailand had been widely criticized for its *lese majeste* laws. In particular, several recent cases – all of which both the Prime Minister and the Fatbook

CEO were very aware -- had raised eyebrows and sometimes cries of alarm and outrage from various quarters, both domestic and international.

To understand more fully the reasons for the lese majeste laws, it was necessary to consider the role and special status of the Thai monarch in Thai culture society.

Monarchs in Thai Culture

Thailand was among the 26 countries in the world that had a functioning monarchy – a "constitutional monarchy," in which the monarch served as head of the state but did not rule [24]. Rather, in matters of governance, the constitutional monarch deferred to the government, which was elected by the majority of people and had the authority to govern. The monarch was under the constitution and had to follow the same law as the people. The countries in this category included the United Kingdom, Belgium, Norway, the Netherlands, Spain, Japan, and Thailand [15]. The second category was that of the "ruling monarchy", where the king ruled the country and chaired meetings of the council of ministers. Countries in this category included most Islamic countries such as Saudi Arabia and Brunei, along with Swaziland, the last absolute monarchy in Africa [15].

Throughout the nearly thousand-year history of the Thai monarchy, the Thai monarch had been imbued with a high religious and social status. In addition, he had close bonds with the people – indeed a monarchy-people bond that was unique among royal houses anywhere in the world, who both loved and respected him for the monarch's contribution to their lives [15]. Hence, although the actual power of the King as head of state was limited to being a symbolic figurehead, the institution itself commanded great respect and reverence by the people [16]. The lifelong accomplishments of the present king, HM King Bhumibol Adulyadej, the world's longest-reigning monarch, had earned him the endless affection and loyalty of his subjects. Unlike many royal families around the world, King Bhumibol had committed himself to improving the lives of the people of his country. During his 64-year-long reign, the King had accumulated a long list of royal national projects, ranging from education to health to agriculture to water management, etc. The King and the royal family had become symbols of Thai national identity. Their portraits were often displayed prominently in almost every home and office building. The King's and the Queen's birthdays were national holidays [17]. Thus, it was important to understand that for most Thai people, the *lese majeste* offence meant not just harm to the monarch but also to the institution and society themselves [15].

Of particular noteworthiness, however, was His Majesty the King's own views of the nation's lese majeste laws as revealed in his lengthy remarks of the 4th December 2005, when he stated in these exact words: *". . . under the constitutional monarchy, the King can do no wrong. Actually, to say that the King can do no wrong is an insult to the King because why can the King do no wrong, . . . this shows that the King is not human. But the King can do wrong . . . . "*

Elaborating, His Majesty was quite clear that as far he was concerned the King was *not* above criticism and indeed and in fact *could be* criticized. He continued with these exact words:

> *But when we say do not criticize, do not violate [the King] because the Constitution says so, in the end the King is troubled. It means that if the King cannot be criticized, that if the King must be criticized, must be violated but cannot be violated, then the damage is done to the King, the King is not a good person. If Thai people, firstly, do not dare and they, secondly, love the King, they do not want to violate. But foreigners often violate the King, and they laugh at the King of Thailand that he cannot be violated, that the king is not a good person, . . . "*
>
> *"... Actually, they should be put in jail. But because foreigners said so, they are not put in jail. No one dares send people who insult the King to jail because the King will be troubled. They accuse that the King is not a good person or at least is sensitive. When someone insults him a little, he told to send them to jail. Actually, the King has never told anyone to send them to jail. Under previous kings, even rebels were not sent to jail, they were not punished. King Rama VI did not punish rebels. Until the time of King Rama IX, who were rebels? There had never been any. Actually, I do the same thing:* ***do not send people to jail but release them. Or if they are in jail, release them. If they are not in jail, do not sue them because it would cause trouble.*** *The person who is insulted is troubled.*
>
> *People who violate the King and are punished are not in trouble.* ***The King is.*** *This is also strange. Lawyers like to launch suits, arrest people and send them to jail. So the lawyers teach the prime minister to sue, to punish. So I tell the prime minister who tells him to punish, do not punish. To punish is not good. In the end, it is not the prime minister who is in trouble.* ***The King is in trouble.*** *Or maybe someone wants the King to be*

in trouble. I do not know. They commit wrong. They insult the King in order that the King is in trouble. And truly the King is in trouble. When people insult us, do we like it? We do not. But if the prime minister punishes them, then it's not good . . . ."[15]

Alas, notwithstanding the King's views on the matter, the law allowed (someone would say "encouraged") the police and indeed *anyone* to pursue a *lese majeste* accusation with nearly complete abandon [15]. The ongoing consequence had been a number of *lese majeste* cases that had been deeply troubling to some observers – Thai as well as foreign -- of the manner in which the law was being applied.

The Case of Joe Gordon

In 2011, a Thai-born American named Joe Gordon was arrested at Suvarnabhumi International Airport as he entered the country for medical treatment. His offense: Translating part of a banned biography of King Bhumibol Adulyadej and posting it on the Internet. Initially, he had thought that surely there had been some mistake. After all, he was domiciled in the United States at the time of the alleged act of *lese majeste. "But, I am an American citizen, and what happened was in America,"* he protested. Unfortunately for him, the position taken by the Thai government official was that the Computer Crime Act applied to anyone, *including foreigners committing the offence outside the country* [18].

Post-sentencing, the U.S. consul general in Thailand, Elizabeth Pratt, was quoted as opining a sentence that *"Washington considered . . . severe because it had been imposed for his exercising his right to freedom of expression."* Her comments were not well received. Within days thereafter, fervent supporters of the Kingdom's *lese majeste* law organized a several-hundred-person protest demonstration at the U.S. Embassy in Bangkok, at which marchers could be heard admonishing the Embassy to "stay out of Thailand's internal affairs" and "mind your own business."

The Case of Alleged Stock Market Manipulators

In mid-October 2009, Thai stock prices fell for two consecutive days, following rumors posted on the Internet that King Bhumibol's health had deteriorated after he was hospitalized in mid-September. The King had thereafter made several public appearances on various occasions. As of late April 2011, he remained in the hospital.

In November 2009, Thai authorities arrested four staff members at KT-Sefigo, Ltd., and the chief executive officer of The UBS securities (Thailand) Ltd., under Section 14 of the Computer Crime Act for posting the false data into a computer system which was deemed likely to damage

national security or to cause a public panic [11]. Ms. Teeranun Wipuchanin, a former UBS employee, and Katha Pajajiriyapon, who worked for local broker KT Zmico Security were arrested. Ms. Teeranun protested that she had only translated a news from a Bloomberg website and posted it on a popular online forum, Prachatai.com. Ms. Teeranun stated that "Everybody on that day wanted to know what caused the market to fall. [But], the stock market had already dropped and we did the translation in the evening". In addition, Mr. Katha was also linked to the Bloomberg article, but he had also added his own comments when posting on the Fah Diew Kan website. Both Ms. Teeranun and Mr. Katha were charged under the Computer Crimes Act [19]. Both had only translated the article from the trusted source that they innocently believe to be true.

The Case of Ampon Tangnoppakul

Another case that had caused controversy so acute that it continued to smoulder even after the convict had passed away was that of a sixty-one-year-old grandfather, Ampon Tangnoppakul, a goods container driver from Samut Prakan who was arrested in mid-2011 on charges of *lese majeste*. Known by many in Thai as Ah Kong (meaning "grandpa") or in English as "Uncle SMS," his alleged crime was to send derogatory text messages about the royal family to a certain government official. The messages were considered by a court to be offensive to the monarchy. Mr. Ampon denied all charges, claiming that he did not know even how to use SMS and that someone else (he knew not whom) had sent the messages and made it seem that they were his. Notwithstanding his impassioned plea to the court, he was found guilty as charged and sentenced in November 2011 to 20 years in prison. Hearing the lengthy sentence, *20 years in prison!,* Mr. Ampon had collapsed in court. Not in the best of health even at the time of his earlier arrest, his health deteriorated rapidly in the aftermath of his incarceration. He died in a Bangkok prison hospital on May 12, 2012.

Mr. Ampon's case provoked intense concern and discussion over what seemed to be the increasingly severe application of the *lese-majeste* laws, in Thailand's criminal code and the Computer Crime Act [20]. Many felt that under the circumstances (e.g., the absence of incontest-able proof that he had sent the text messages, as opposed to someone else -- someone who may have had access to his phone), a 20-year sentence, which in the case of a 61-year-old person was tantamount to a *life sentence*, was somehow not quite right. His case continued to gnaw at the conscience of many throughout the society.

Amidst what were considered to be increasing incidents of anti-monarchy content on websites, the duly authorized government authorities, operating under what many described as the strictest *lese majeste laws* of any monarchy on the planet, had taken to aggressively shutting down websites. A Thammasat University study reported that the courts had used the Act to block nearly 75,000 web pages, of which 57,330 were shut down due to alleged anti-monarchy content. Some 44,000 of those blocked pages were blocked in 2010 [14].

It was precisely because of incidents such the several cited hereinabove that the two decision makers, Prime Minister Shinawatra and CEO Dungen, continued to ruminate – and fret – over what might be the best courses of action for the separate decisions that each had to make. Dungen certainly had no desire to find himself apprehended while going through Immigration formalities during some future visit to the Kingdom and unceremoniously hauled off to jail. And, for her part, Khun Shinawatra, had no desire to see such laws scare off the very investors on whom she was depending to help bring in the foreign direct ICT investment that Thailand needed to become the "Wisdom and Learning Society" that she believed was essential to the nation's long-term competitiveness. For these reasons, both decision makers were nearly at a loss as to decide what course of action would advance their objectives, while minimizing their risks.

The Case of Dr. Somsak Jeamteerasakul

Dr. Somsak Jeamteerasakul, an associate professor of history at Thammasat University in Bangkok, was arrested on 22nd April 2011 under a lese majeste charge. Dr. Somsak was an avid critic of the lese majestic law and was calling for reform of the monarchy. Dr. Somsak was a frequent speaker on public forums, both online and offline. He frequently posted his comments on his Facebook and other public websites [21-22]. After the arrest, he insisted that

> *"I have never talked about overthrowing the system -- only changing the system to reflect a changing world. Open discourse about the role of the monarchy is necessary . . . . We should have a debate on the role of the monarchy, using reason and evidence . . . . To royalists, I ask: "What will you do with the millions of different views?"* [22]

Several journalists and academics subsequently signed an open letter calling on the authorities to drop charges against Dr. Somsak and bring to an end the restriction of freedom of speech. They wrote: *"Those in power must realize that discussion and criticism – not blind loyalty – are*

necessary in a functioning democracy." [22]

Because the *lèse-majesté* laws were very broad, with a low burden of justification for charging a person with a violation, it opened the door to allegations by citizens with ulterior motives. That is, it created a situation in which any citizen could accuse another of making comments that allegedly "insulted" the King and/or the members of the royal family. Most victims did not know who had accused them [23]. With very little substantive justification required to charge a person under the *lese-majeste* law, prosecutions under the law had increased incessantly. The National Human Rights Commission's Subcommittee on Political and Civil Rights assessed that there were more than 400 *lèse-majesté* cases prosecuted under article 112 of the Penal Code and article 14 of the Computer Crime Act in 2010. Most cases were closed to the public [24]. According to statistics on computer crime released by the Technology Crime Suppression Division, the total 73 cases in 2010 had grown exponentially to 431 cases in 2011 [11]. Most cases involved inputting inappropriate content related to the "kingdom security" (See Table 1).

Holding Internet Service Providers Accountable

Another controversial provision of the Act pertained to Section 15, which allowed authorities to charge any ISP or service provider that intentionally supported or consented to the commission of an offense under Section 14. The service providers included website and webboard owners that hosted material prohibited by Section 14 (See Appendix 7). Several critics had argued, vigorously, that ISPs and service providers should not be subject to the same penalty as the primary offenders because they only provided technical service and did not create the (illegal) content.

When that argument fell on deaf ears, industry participants and observers alike had known that it was but a matter of time before some website or webboard owner found themselves on the wrong side of the law. They had not had to wait long. On March 6th, 2009, Ms. Chiranuch Permchaiporn, 44 years old, the web master of Thailand's popular Prachathai news website, was arrested by the Crime Suppression police and charged under section 15 of the Act. Her crime: The failure to remove quickly enough offensive comments posted by an anonymous user. According to the Financial Times, Ms. Permchaiporn argued that the Act had "created a climate of fear." *"I didn't say anything, I didn't write anything, I didn't post anything," she protested. "But as webmaster [editor]. I am facing the penalty"* [25].

The Chiranuch case had potential implications for Internet giants such as Google and Facebook. John Ure, executive director of the Asia Internet Coalition, a trade association-cum-pressure group set up by Google, Ebay, Skype and others, was quite emphatic about what Chiranuch's conviction would mean with respect to the future prospects of the industry in Thailand. *"If they [Internet access providers] are found to be liable, it would be very detrimental to the whole digital economy of Thailand,"* he stated. *"E-commerce, social networking and the like would all be completely disrupted"* [25]. Further, although he did not say so (he didn't need to), industry observers understood that such disruption would diminish considerably Thailand's future prospects of attracting additional direct foreign investment from any of the members of this, and possibly other similar industry groups.

The Cost of Compliance with the Demands of the Act

Section 26 of the Act specified that service providers must store computer traffic data for at least ninety days from the date on which the data was input into computer systems. (See Appendix 6 for definitions of the four different categories of service providers covered under this section of the Act.) The section also stipulated that, if needed, authorities could order service providers to store computer traffic data for a longer period but not more than one year. Under this section, the service provider was obliged to store the necessary information to enable identification of the user of the service. The purpose of this section was to facilitate law enforcement's gathering of evidence pertaining to an offence and tracing the identity of the offenders. In other words, the intent of this section was to prevent anonymous use of the Internet.

The requirements of this section elevated appreciably an ISP's cost of doing business, especially for small and medium-size enterprises (SMEs) because of the investment in systems (hardware and software) to keep computer traffic log files of data. The software alone could cost around 100,000 baht (approximately US$ 3,400). The cost of a whole system could range between one and ten million baht (i.e., US$ 34,000 to US$ 340,000) [26]. Sawatree Suksri, a professor of Internet and media law at Bangkok's Thammasat University pointed out that "the hardware and software required to store all computer traffic would be extremely costly [18]." However, a failure to comply could also be costly, as the Act stipulated that any service provider that failed to comply would be subject to a fine of to 500,000 baht (approximately US$ 17,000) *for each offense*.

Fatbook and CEO Dungen's Concerns

All of the foregoing issues were of enormous concern to Tom Dungen. Following his 2004 launching of Fatbook, his social network website had grown rapidly to become one of the major websites of its genre by 2012. As of May 2012, Fatbook had over 900 million active users, more than half of them accessing the service using mobile devices. Users had to register before using the site, after which they could create their own profile and link other users as friends. The website enabled users to communicate and exchange messages, including photos and videos, with their friends. Moreover, users could join common-interest user groups that had similar interests, e.g., the rock 'n roll, travel, sports car enthusiasts user groups, etc. -- to cite a few examples. Advertising and selling of online items were Fatbook's main source of revenue, which had been growing, albeit not at the same fast clip as registered users.

Fatbook's phenomenal success in the North American and European social website markets had stalled in the Chinese and Russian markets due to conflicts with the two respective governments that had led to Fatbook's eventually exiting those countries. The major conflicts usually involved governmental violation of basic human rights, such as the right of free speech. Also, in some countries such as China, the law required the website owners to disclose customer's information to the government. Rather than violate what it viewed as a "sacred vow' to its users to maintain the confidentiality of their identity, Fatbook voluntarily withdrew from those markets.

Recently, Fatbook had then begun to direct its expansion intentions to developing countries. Thailand was chosen as the destination for the company's second foray into developing countries, China and Russia having been the initial points of entry. As the most popular website in Thailand, Fatbook's number of registered Fatbook users and advertisers was steadily growing. Almost 90% of Internet users in Thailand had Fatbook accounts. Hence, it was believed that having Fatbook in Thailand would be a win-win situation both for Thai Internet users and Fatbook. Further, the successful launch of a Thai version of Fatbook, the firm would gain invaluable experience with which to penetrate other potentially lucrative national markets in the Asian region, e.g., Indonesia, India, South Korea, and Japan.

However, the Computer Crime Act of Thailand, as currently promulgated and enforced, had two provisions that were sufficiently troubling and unpalatable as to make Dungen wonder whether Thailand was the best choice for the firm's new foray into developing countries.

Worries about Section 15 of the Act

First, because Fatbook allowed its users to create and share content, the provision of Section 15 of the Act – which made website and webboards equally culpable in instances where a user posted content deemed illegal under Section 14 of the Act – was a virtually unshakable worry. He kept thinking about the case concerning the Thai webmaster, Chiranuch Premchaiporn, who at a youthful 44 years old, was on trial for allegedly violating Section 15 of the Act by being "too slow" to delete antiroyal content on the popular Web forum that she ran. If convicted, she faced 20 years in prison [18]. Dungen couldn't help but shudder as he contemplated the thought he might end up in Ms. Chiranuch's predicament.

Another concern was that several countries in the region were preparing to follow Thailand's lead in imposing liability on website owners for illegal comments posted by website visitors. For example, Vietnam was preparing to extend its "anti-criticism" law to make it illegal for any website, including blogs and social networks, to criticize the ruling Communist Party or to set up any website, where a visitor could post antigovernment content. In Malaysia, website owners could be presumed guilty if any illegal material was uploaded to their websites [27]. The trend had even recently leapt from Asia and Russia to Latin American developing countries, where (for instance) a Brazilian elections court issued an arrest warrant against Google's highest senior executive in the nation because the company had neglected to remove YouTube videos criticizing a local mayoral candidate [28]. In Brazil, the law prohibited campaign ads that defamed a candidate. Google responded that *"Google believes that voters have a right to use the Internet to freely express their opinions about candidates for political office, as a form of full exercise of democracy, especially during electoral campaigns"* [28].

Worries about Section 26 of the Act

A second cause for concern was the requirement of Section 26 of the Act that imposed on ISPs a duty to collect and store computer traffic data for 90 days. A company was required to turn in computer traffic data to the authorities if any actionable violations of any provisions of the Act were believed to stem from the company's network. For example, if illegal content were created and shared on Fatbook's website, Fatbook would need to turn in computer traffic data that indicated who the users were. From its inception, however, Fatbook had adhered to a policy of non-disclosure. That is, its privacy policy promised users that the firm would not disclose any private information pertaining to its users. It was a policy of which Fatbook was especially proud because it created a bond

of trust between the firm and its website users. There was no question in Dungen's mind but that the act of turning customers into the authorities would have a deleterious impact on the growth of new users and quite possibly a desertion by an unknown number of current users.

Prime Minister's Perspective and Concerns

As prime minister, Khun Yingluck had been exposed to impassioned arguments on both sides of the issue. She also knew that there were points well taken by both the pro- and anti-Computer Crime Act partisans. Reviewing in her mind the arguments against the Act, the Prime Minister could not deny that the Act was impeding freedom of expression and international investment; but, at the same time, she also realized that the Act was the only tool for the authorities to prevent and deter computer crimes.

She was also familiar with the command of the Thai Constitution (Section 8) that: *"The King shall be enthroned in a position of revered worship and shall not be violated. No person shall expose the King to any sort of accusation or action."* In large part because of his many decades of wondrous works on behalf of the people and nation, profound reverence for the King was deeply embedded in the psyche of the Thai people. Insults to the king or royal family were viewed, and treated, as a threat to national security. In the words of Thitinan Pongsudhirak, a political scientist at Bangkok's Chulalongkorn University: *"If you say 'we want a monarchy but we want reform', you provoke a hysterical reaction. It forces people into antimonarchism"* [25]. Of all of these facts, the Prime Minister had long been aware.

On the other hand, Khun Yingluck was also aware of the persistent claims of human rights activists, academics, and many ordinary Thai people that the *lese majeste* laws were increasingly being used as a tool to lock up political opponents instead of protecting the monarchy [25]. Indeed, data collected by David Streckfuss, an academic who had conducted comprehensive research on the use of *lese majeste* in Thailand, had found that the number of *lese majeste* prosecutions had increased 15-fold between 2005 and 2010 [25]. This was also the period of some of most intense political conflict that the country had witnessed since the early-1990s. The Prime Minister could not altogether dismiss the possibility that the two phenomena – i.e., political and societal conflict and the increase in prosecutions under the *lese majeste* laws – were fundamentally related.

Apart from these concerns, several additional considerations were uppermost in the Prime Minister's mind. These were the impact of the

Computer Crime Act on Thailand's access to needed foreign direct investment; the related issue of international views and opinions; and, last but not least, the all-important perspectives of the law enforcement community in Thailand.

Concerns about the Impact on Foreign Direct Investment

With her business background in the telecommunications industry, Khun Yingluck understood that in developing countries, the way to upgrade business was through attracting foreign investment. Foreign direct investment (FDI) benefited both the investing organization and the host nation. That is, the investor gained the advantage of cheaper wages and access to a new market new talent, while the host nation gained an inflow of foreign capital and investment funds, along with the transfer of best practices, skills, and technology [29]. Because of its potential, as Michael Porter noted, to boost a nation's competitiveness, developing countries competed to develop and sustain a good business environment with which to attract FDI. Fundamentally, then, the goal of FDI attraction was to boost a nation's prosperity through upgrading competitiveness [30] – a situation that could enhance the Prime Minister's overriding objective of developing Thailand into a "Wisdom and Learning Society" able to compete with the best. Thus, any impediments to the attraction of needed FDI warranted ongoing, concerted attention.

Concerns about International Pressures

A second, and a related concern, was the views of the larger international community – i.e., Thailand's image among the community of nations. Clearly, the state of the country's image on the international stage would ultimately have an impact – positive or negative – on, among other things, the inflow of foreign direct investment. In this connection, the Prime Minister had to factor into her decision the recent criticisms that several international groups had placed in the public domain in consequence of the promulgation and operation of the Computer Crime Act. For example, free-speech activists, positing that the authorities had blocked at least 110,000 websites in 2010 due to their supposed anti-government or anti-monarchy content, had taken up the refrain that Thailand was becoming one of the least-free states in Asia, joining China and Myanmar when it came to the freedom on the Internet [12].

Further criticism had come from closer international quarters. Pavin Chachavalpongpun, a Thailand expert at the Institute of Southeast Asian Studies in Singapore, exclaimed that Internet censorship in Thailand had reached "an unprecedented level". He went on to state that "The government has been using this partly to defend national security but also

to protect its own regime as well" [12]. In addition, the influential Human Rights Watch had declared that Thailand's Internet censorship was "a broad-brush clampdown that violated Thailand's obligations to respect media freedom and freedom of expression" [12].

The chorus of criticism did not stop there. Others had critiqued specific provisions of the Act and found them, in their view, ill-advised. For example, concerning the *lese majeste* laws, a senior western diplomats had been quoted in the *Financial Times* as saying,

> *"There's nothing wrong with the idea of a country respecting and honouring their monarch. What is troubling is to see a government use laws designed to protect an important institution like the monarchy in a way that exacerbates social divisions, or excessively punishes those who have expressed their criticisms* [25]*".*

Several international businesses had weighed in on Sections 15 and 26 of the Act. The earlier quoted Hong Kong-based Asia Internet Coalition – comprised of Google, Yahoo, eBay, Nokia Corporation, and Microsoft – added to their earlier criticism of the Chiranuch Premchaiporn webmaster case. *"By holding an intermediary liable for the actions of its users, this case could set a dangerous precedent and have a significant long-term impact on Thailand's economy," the group stated* [18]. The group also warned that *"Changing the way the Internet works in Thailand by denying intermediaries the protections they are granted in most countries around the world could have a significant detrimental impact"*[18].

The Prime Minister knew that these criticisms were unlikely to abate. In fact, absent changes in the Computer Crime Act to address the concerns of these groups and individuals, it was quite likely that their protests against the law would expand and be amplified.

Concerns about Law's Enforcement's Perspective

Khun Yingluck sighed as she reflected on the possibility that the concerns of sources of foreign direct investment and international critics of various types might have been rather easily addressed, but for the fact that the Computer Crime Act proponents and defenders who were no less influential and vocal in their support than were the critics and opponents. That is, juxtaposed against the voices of dissent was the vast Thai law enforcement community for whom the law had been something of "godsend."

More specifically, following its 2007 legislative passage, the Computer Crime Act had become a major tool for law enforcement to

combat computer crimes, with law enforcement enjoying vast new power under provisions of the Act. For example, with the power granted under Sections 18 and 26 to investigate and gather evidence of an offense committed by or via the computer, data or computer traffic data from any suspected computer systems could be easily accessed to gather evidence. Authorities could also demand passwords and decode any individual or organizational data and confiscate any computer system for up to 90 days as part of their investigation [31]. Finally, they felt, they had the means to track down and bring to account persons guilty of various types of computer-based crime.

If anyone had expected law enforcement to be bashful in the use of their new powers, they were sorely disappointed. To the contrary, law enforcement claimed that they needed to have this power to be able to investigate crime. They also maintained that computer and Internet crime was different from traditional crime. In cyber crime, the pointed out, offenders could be anywhere in the world, making it exceptionally difficult to gather evidence because of the complexity of computer systems and the Internet. It was also difficult to prosecute offenders because cyber crime could involve many national jurisdictions. For example, offenders could be in the US, the server that stored illegal data could be in Europe, while the impact of the crime could be in Thailand.

Not only had the 2007 Computer Crime Act enforced penalties for illegal activities on the Internet, authorities claimed that it had also been designed to tackle fraud, as e-commerce developed in the country. Further, concerning the criticism of the *lese majeste* provisions of the Act, the authorities noted that strict *lèse-majesté* rules limiting discussion of the monarchy dated back several centuries and thus was nothing new [12]. Noting further that the Computer Crime Act in Thailand was very different from its counterparts in the US and Europe, Thai law enforcement maintained that national security should come before the country's competitiveness and freedom of expression. In brief, far from seeing a need to amend the Act to address the criticisms of concerned others, law enforcement's perspective was that, if anything, the Act needed to be amended to make the punishment *harsher* and more extensive, and to give more power to law enforcement.

If she had had any doubt whatsoever about just how contentious the issue of amending or not amending the Act would be, the views of the law enforcement community completely eradicated it. Heaving another - sigh, the Prime Minister slowly shook her head as the full extent of her "catch-22" dilemma dawned on her. Clearly, she thought to herself, the *lese majeste* laws – the core issue of contention -- were a highly sensitive matter

in Thailand, placing her in a "damned-if-I-do, damned-if-I-don't conundrum. Interfering with the law would be interpreted by her opponents as a sign of disloyalty to the king and the royal family, a severe charge. *How* severe a charge it could potentially be was evident in the 2006 military ouster of her brother and former prime minister, Thaksin Shinawatra, who was removed from office under the accusation of *lese-majeste* for comments he made about the monarch in newspaper interviews [21].

But, on the other hand, if she refused to try to amend the law, Thailand's reputation and standing among the community of nations and its access to the direct foreign investment needed to propel the vision of a "Wisdom and Learning" society would likely suffer. But, if she attempted to amend the law to make it more palatable to the critics and international bodies, she could get herself and her cabinet in a very dangerous position, as the law enforcement community had subtly insinuated.

Decision Options

Both the Prime Minister and Tom Dungen faced difficult decisions. There were four decision alternatives that could potentially affect Thailand, as well as Fatbook. They were:

Alternative 1: The Prime Minister and her government decide to amend the Computer Crime Act, and Tom Dungen decides to launch Fatbook in Thailand.

This alternative would be beneficial for Fatbook since it would lower the risks and provide financial gain for the company. Thai Internet user would enjoy specialized services and support from Fatbook. However, the Prime Minister and her government incur weighty political risks, and computer crimes and inappropriate content might well rise.

Alternative 2: The Prime Minister and her government decide to amend the Computer Crime Act and Tom Dungen decides not to launch Fatbook in Thailand.

This alternative would not be beneficial to either the Prime Minister or Dungen. Dungen might choose this alternative because he believes that uncertainty still exists in the law, but in any case he foregoes the prospect of increased revenues and profits. The Prime Minister and her government might incur high political risks for amending the law.

Alternative 3: The Prime Minister and her government decide not to amend the Computer Crime Act and Tom Dungen decides to launch Fatbook in Thailand anyhow.

This alternative would introduce high risks but also provide financial gain for Fatbook. The Prime Minister and her government would incur low political risk, but the country's image would continue to be damaged.

Alternative 4: The Prime Minister and her government decide *not* to amend the Computer Crime Act and Tom Dungen decides *not* to launch Fatbook in Thailand.

This alternative would have little or no immediate risk for either the Prime Minister or Dungen. However, Fatbook would lose those additional revenues and profits that would accrue from adapting Fatbook to the Thai market, and Thailand's image would continue to be damaged.

Endnotes

1 NECTEC, Thailand ICT Market. 2009, Software Industry Promotion Agency National Electronics and Computer Technology Center.

2 NSTDA, Thailand ICT Market and Outlook. 2011, National Science and Technology Development Agency.

3 Santipaporn, S. Information and Communication Technology Statistics in Thailand. in International Seminar on Information and Communication Technology Statistics. 2010. Seoul, Republic of Korea.

4 Forum, W.E., The Global Competitiveness Report 2011-2012 2012.

5 internetworldstat.com. Asia Internet Usage and Population 2011 Jan 2]; Available from: http://www.internetworldstats.com/stats3.htm.

6 ThaiCert, Year 2007 ThaiCERT's handled Incident Response Summary, N. Sanglerdinlapachai, Editor. 2007, Thai Computer Emergency Response Team.

7 Putnam, T.L. and D.D. Elliott, International Responses to Cyber Crime, in The Transnational Dimension of Cyber Crime and Terrorism, S.E. Goodman and A.D. Sofaer, Editors. 2001, The Hoover Institution Press.

8 Smith, R. and G. Urbas, Controlling Fraud on the Internet: A CAPA Perspective. 2001, Australia Institute of Criminology

9 Annoymous, UN Rights Chief Dismayed By Harsh Sentencing Of Vietnam Bloggers in RTTNews. 2012.

10 Asia, B., Vietnam prime minister targets anti-government blogs, in BBC. 2012.

11 Apichanont, A., Country Report. 2011, Technology Crime Suppression Division: Bangkok, Thailand.

12 Barta, P., Thai Groups Denounce Website Censorship; Government Blocks Thousands of Pages Following Clashes, in Wall Street Journal 2010, Wall Street Journal: New York, N.Y.

[13] Tunsarawuth, S. and T. Mendal, Analysis of Computer Crime Act of Thailand. 2010.
[14] Annoymous, Asia: When more is less; Thailand's monarchy, in The Economist. 2011.
[15] Uwanno, B., "Lèse-majesté": A Distinctive Character of Thai Democracy amidst the Global Democratic Movement. 2012, The King Prajadhipok's Institute.
[16] Wikipedia. Monarchy of Thailand. 2012 [cited 2012 Jan 3rd]; Available from: http://en.wikipedia.org/wiki/Monarchy_of_Thailand.
[17] Aquno, M. Thailand's Strict "Lese Majeste" Laws - The Thai Reverence for the King 2012 [cited 2012 Jan 12]; Available from: http://goseasia.about.com/od/thaipeopleculture/a/lesemajeste.htm.
[18] Hookway, J., U.S. Man's Jailing Spotlights Thai Monarch Law, in Wall Stree Journal. 2011: New York, N.Y.
[19] Johnston, T., Two charged over Thai king rumours, in Financial Times. 2009: London (UK).
[20] Annoymous, An inconvenient death; Thailanwd's lese-majeste laws. 2012, The Economist. p. 47.
[21] Johnston, T., A divisive dynasty, in Financial Times. 2011, Financial Times: London, UK.
[22] Gardner, L., Somsak: "what I'm facing is scary". 2011, Australia National University.
[23] Coz, C.L., Could Facebook, Twitter Be Charged Under Thailand's Computer Crime Act?, in PBS. 2012.
[24] Annoymous, Thailand: End Harsh Punishments for Lese Majeste Offenses. 2012, Human Rights Watch.
[25] Johnson, T., Draconian Thai law lands editor in court over online posting, in Financial Times. 2011: London (UK).
[26] Annoymous, Log Files and Computer Crime Act, in Thanonline.com. 2008: Bangkok.
[27] Hookway, J., Conviction in Thailand Worries Web Users, in Wall Street Journal. 2012, Wall Street Journal: New York, N.Y.
[28] Haynes, B., Google executive in Brazil faces arrest over elections law, in Reuters. 2012, Reuters: Sao Paulo.
[29] Wikipedia. Foreign direct investment. 2012 [cited 2012 Feb 12]; Available from: http://en.wikipedia.org/wiki/Foreign_direct_investment.
[30] Porter, M.E., The competitive advantage of nations : with a new introduction. 1998, New York: Free Press. xxxii, 855 p.
[31] Singh, A., Thailand's Computer Crime Act still a major threat to free expression. 2010, Thailand Business News.