June 22, 2016

National Legislative Assembly
U-Thong Nai Road
Dusit, Bangkok
Thailand 10300

Dear Sir/Mdm,

The Asia Internet Coalition (AIC) would like to respectfully provide comments to the draft amendments to the Computer-related Crime Act (CCA) that is currently under review by the Ad Hoc Committee on the Computer-related Crime Act B.E. … of the National Legislative Assembly (NLA).

The AIC is a policy voice of the digital industry in the Asia-Pacific comprising Apple, Facebook, Google, LinkedIn, Twitter and Yahoo!. Our aim is to ensure that the policy and regulatory environment for the industry will allow users to enjoy the maximum economic, social and cultural benefits from the online world in the years ahead, and that they can do so safely, securely and confidently.

The AIC commends the Kingdom of Thailand for recognizing the importance of the digital economy to economic growth and shares the government's aspiration for Thailand to emerge as a digital hub for the region. In particular, we note the Royal Thai Government's 20-year digital economy master plan aimed at promoting digital commerce, digital entrepreneurship, digital innovation and digital content, and recent initiatives to support Thailand's budding start-up scene.

Thailand is situated in one of the most vibrant corners of the global digital economy. A recent study by Google and Temasek released this month sees the region's Internet economy (including Thailand) reaching US$200 billion (7.4 trillion baht) by 2025, with e-commerce alone exceeding US$88 billion (3.1 trillion baht) with the potential to reach US$120 billion (4.2 trillion baht).[1]

To achieve this potential, however, requires governments to put in place the right conditions to support investment and nurture innovation in the digital economy. The same study estimated that about US$40-50 billion (1.4-1.7 trillion baht) in investments will be needed for Southeast Asia to fulfil the growth potential of its Internet economy. A separate study by Fifth Era released in January this year found that investors are highly sensitive to regulatory uncertainty and developments when deciding to invest in Internet businesses.[2]

In light of this, in amending the CCA, AIC hopes that the Royal Thai Government uses the opportunity to update the law to strengthen users' trust for online services by enhancing the safety and security of the online environment, as well as provide legal certainty for investors, online services and content creators.

---

[1] e-conomy SEA: Unlocking the US$200 billion digital opportunity in Southeast Asia. *Google and Temasek*. June 2016. http://goo.gl/p7BZ95

[2] The Impact of Internet Regulation on Investment. *Fifth Era*. January 2016. http://goo.gl/71g7zN

AIC member companies provide some of the platforms and tools that contribute to an increasingly digital global economy, and that facilitate e-commerce and grow new digital industries in individual economies such as in Thailand. We stand ready to share our knowledge and insights on ways governments can nurture and protect an innovative and dynamic digital sector.

In this spirit, we respectfully submit our comments to the draft amendments to the CCA and hope that you consider them favorably. The members of AIC remain at your disposal to discuss these matters in greater detail.

Sincerely,

Hans Vriens
Secretariat, Asia Internet Coalition

AIC's Comments to Draft Amendments to Computer Crimes Act (CCA)

1. Section 9: Intermediary Liability

In the proposed amendments to Section 15 of the CCA, AIC is concerned about the lack of clarity on liability protections for Internet intermediaries.

Internet-based services that facilitate interaction between people and businesses online are considered Internet intermediaries, and they include members of AIC as well as home-grown Thai online services. In this regard, intermediaries are an important part of the digital economy and support broader economic growth. Indeed, a 2010 OECD study found that intermediaries support employment and economic growth, lower barriers for businesses and reduce costs for consumers.[3]

Internet intermediaries should not be held liable for content generated on their platforms by their users. The lack of clarity in Section 15 in this regard could have a deterrence effect on future investment in intermediaries in Thailand, as well as raise barriers for new such start-ups. A Fifth Era report released in January 2016 found **71% of investors surveyed were uncomfortable investing in markets where intermediaries could be held liable for third-party actions or content**. A separate study on the economic impact of liability limitations on start-ups concluded that **clear and cost-efficient requirements for intermediaries could increase start-up success rates in Thailand by 24%**.[4]

Recommendation: AIC respectfully recommends that **a clear safe harbour provision for Internet intermediaries should be included in the proposed amendments to Section 15 of the CCA**.

2. Section 8: Definition of Computer Crimes

In the proposed amendments to Section 14 of the CCA, AIC is concerned about the unclear definitions of what constitutes a computer crime. In particular, the definition of crimes defined as those that involve input of computer data that "cause injury to national security, public safety, economic security, or infrastructure for the public interest, or public panic" or that constitute "obscene computer data which is likely to be accessible to the public" are overly broad.

These vague definitions bear the risk of stifling freedom of expression and the creative economy in Thailand, as well as creates legal uncertainty, which in turn deters investment. The aforementioned Fifth Era report consistently found that **over 75% of investors surveyed since 2011 reported regulatory ambiguity as having a chilling effect on investment**. A similarly high proportion of investors **(79%) were uncomfortable investing in markets where freedom of expression is restricted or highly regulated**.

Recommendation: AIC respectfully recommends that **these definitions of computer crimes should be defined more clearly.**

[3] The Economic and Social Role of Internet Intermediaries. *OECD*. April 2010. http://goo.gl/9KMcwU
[4] How are Internet Start-ups Affected by Liability for User Content? *Oxera*. 2015. http://goo.gl/AdzJnu

3. Access to Computer and User Data

AIC members take seriously their responsibility to maintain the safety, privacy and security of the users of their products. They recognize that there are many situations where it is in the interests of people using their service that law enforcement agencies carry out an investigation into suspected criminal activity. Most large, global online service companies, including AIC members, already have developed and implemented proven voluntary processes for disclosing account records in accordance with terms of service and applicable laws. These processes work efficiently on a global scale, and are being used by governments around world.

Recommendation: AIC notes that Section 19 of the CCA provides for the authorities to first obtain a court order, with relevant jurisdiction, before they can access data or order service providers to share that data, including user data, to conduct investigations. **AIC recommends that this requirement be retained in any amendments to the CCA being considered**, and welcomes the opportunity to discuss our companies' processes in greater detail. **AIC also recommends that Section 18(7) of the CCA, when referring to "the individual," is clarified to apply to the offender and relevant individual only, and not the service provider or enterprise.**

4. Section 15: Notice and Takedown Procedures

AIC notes that the proposed amendments to Section 20 of the CCA provide for judicial review by "a court with jurisdiction" for requests by the government to block or remove computer data. At the same time, we note that the proposed Section 20(4) provides for the yet-to-be appointed Minister of Digital Economy to "prescribe rules, duration and guidelines for the suspension of dissemination or removal of computer data by the service providers for consistency under changing technological environment".

In practice today, many large, global online service companies, including members of AIC, already have developed and implemented proven voluntary "notice and takedown" processes to allow consumers, organizations and governments to "flag" illegal content and request its removal. These processes work efficiently on a global scale, and are being used by countless individuals, organizations and governments around the clock.

Recommendation: AIC members welcome the opportunity to elaborate on our individual companies' "notice and takedown" processes and community guidelines. **Insofar as government content restriction orders are deemed necessary, AIC respectfully recommends that such orders should be:**

a) specific, clear, unambiguous, and consistent with human rights principles;
b) issued by an independent body that is explicitly authorized to adjudicate on censorship — namely, a judge or other independent authority;
c) directed to the *creator* of content — not intermediaries — except in exceptional circumstance such as when the creator cannot be contacted after repeated efforts;
d) subject to due process (including the right of appeal); and
e) subject to clear rules providing for transparency.

In regard to (a), AIC recommends that **the reference to computer data "in violation of public order or good morals of the people" in the proposed Section 20(4) should be defined clearly.** This is in addition to our recommendation above, that definitions for computer crimes in proposed amendments to Section 14 of the CCA should be defined clearly.

In regard to (c), AIC recommends that **notice and takedown procedures shall absolve Internet intermediaries of liabilities under the proposed amendments to Sections 15 and 20 of the CCA.** This could be stated in a safe harbor provision for intermediaries in Section 15 of the CCA as recommended above.