Analysis of Computer Crime Act of Thailand

By Sinfah Tunsarawuth and Toby Mendel[1]

May 2010

1. Preamble

1.1 The Computer-Related Offences Commission Act, better known as the Computer Crime Act, has been enforced in Thailand for less than three years, and yet it has already created a great deal of controversy and concern. The Thai government has applied the law to shut down or block thousands of websites and to prosecute a number of individuals. It is thus a piece of legislation that has had a significant and negative impact on freedom of expression on the Internet since it came into force in July 2007.

1.2 The law came into force at a time when the Internet had already established itself as a popular means of communication, especially for urban, educated Thai people. The Internet allows for a freer flow of information due to the fact that it is more difficult for the government to control. It also offers alternative sources of news from the rather conservative Thai traditional mass media. The Internet also provides a public forum for ordinary citizens, who do not have easy access to the established media, to express their views and opinions.

1.3 By the end of 2008, there were 13.4 million Internet users in Thailand, almost five times more than the number of users in 2000, according to the 2008 annual report of the National Telecommunications Commission (NTC), the country's telecommunications industry regulator. By the end of the first quarter of 2009, NTC had granted Internet service provider licenses to 113 operators in the country.

1.4 In its report for the first quarter of 2009, NTC noted that the Internet market in Thailand had been expanding dramatically, with a retail market of 6.64 billion baht (approximately US$199.9 million) in 2008, up 44% from a year earlier. The agency predicted at that time that the value would increase by another 28% to 8.51 billion baht (approximately US$256.3 million) in 2009. The report also noted that almost all urban users have now migrated from older dial-up systems to high-speed Internet, although many users in rural areas still use the much slower dial-up access.

1.5 The State-owned TOT Public Company Limited, formerly the Telephone Organization of Thailand, maintained the largest market share in terms of providing high-speed Internet services, with 41.2% of the market share at the end of the first quarter of 2009, followed by two privately-owned companies,

[1] Sinfah Tunsarawuth, the lead author of this report, is an independent media lawyer based in Bangkok, Thailand. He can be contacted at sinfah@hotmail.com. Toby Mendel, who provided international materials for and edited the report, is the Executive Director of the Centre for Law and Democracy, a Canadian-based international human rights NGO focusing on foundational rights for democracy. He can be reached at toby@law-democracy.org.

True Corporation Public Company Limited, at 37.6%, and TT&T Public Company Limited, 20.8%. All the three companies also operate fixed-line telephone networks.

1.6 The dramatic rise in Internet use in Thailand, particularly in urban areas, has been accompanied by a significant growth in the number of websites, both news- and non-news-oriented, and various web boards and blogs. Many educated, middle-class Thais now use these web boards and blogs to express and share their views on social, economic and political issues, as these new channels allow them to publish their opinions by themselves, without having to be screened or censored. This is particularly popular due to the fact that Thai mainstream media have recently been seen as leaning towards the royalist camp in the current political polarisation around the issue of monarchy. Internet publication also travels immediately, and irrespective of borders, to an unlimited number of readers. Users can also remain anonymous. Social networking sites such as Hi5, Facebook, YouTube and twitter have also become increasingly popular among the young urban population.

2. International Standards

2.1 General Standards

2.1.1 Thailand acceded to the International Covenant on Civil and Political Rights (ICCPR),[2] a formally legally binding international human rights treaty which has been ratified by 165 States,[3] on 29 October 1996. Article 19 of the ICCPR guarantees the right to freedom of expression in the following terms:

> 1. *Everyone shall have the right to freedom of opinion.*
> 2. *Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art or through any other media of his choice.*

2.1.2 Freedom of expression is also protected in all three regional human rights instruments, at Article 9 of the African Charter on Human and Peoples' Rights,[4] Article 10 of the European Convention on Human Rights[5] and Article 13 of the American Convention on Human Rights.[6] Judgments and statements issued by courts and other authoritative sources under these regional mechanisms are not directly binding on Thailand, but at the same time they do offer a persuasive interpretation of international freedom of expression principles, which are relevant for Thailand.

2.1.3 Freedom of expression is a key human right, in particular because of its fundamental role in underpinning democracy. At its very first session, in 1946, the UN General Assembly adopted Resolution 59(I) which states: "Freedom of information is a fundamental human right and ... the touchstone of all the freedoms to which the United Nations is consecrated."[7] As the UN Human Rights Committee has said:

> *The right to freedom of expression is of paramount importance in any democratic society.*[8]

2.1.4 At the same time, freedom of expression is not absolute and both international law and most national constitutions recognise that it may be restricted. However, Article 19(3) of the ICCPR lays down strict conditions which any restriction on freedom of expression must meet:

> *The exercise of the rights provided for in paragraph 2 of this article carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only*

---

2 UN General Assembly Resolution 2200A(XXI), adopted 16 December 1966, in force 23 March 1976.
3 As of 19 April 2010.
4 Adopted 26 June 1981, in force 21 October 1986.
5 Adopted 4 November 1950, E.T.S. No. 5, in force 3 September 1953.
6 Adopted 22 November 1969, O.A.S. Treaty Series No. 36, in force 18 July 1978.
7 14 December 1946. This Resolution refers to freedom of information in its broad sense, as the free circulation of information and ideas.
8 *Tae-Hoon Park v. Republic of Korea*, 20 October 1998, Communication No. 628/1995, para. 10.3.

be such as are provided by law and are necessary:

a) *For respect of the rights or reputations of others;*
b) *For the protection of national security or of public order (ordre public), or of public health or morals.*

A similar formulation can be found in the ACHR and ECHR. These have been interpreted as requiring restrictions to meet a strict three-part test.[9] International jurisprudence makes it clear that this test presents a high standard which any interference must overcome. The European Court of Human Rights has stated:

> *Freedom of expression … is subject to a number of exceptions which, however, must be narrowly interpreted and the necessity for any restrictions must be convincingly established.*[10]

2.1.5 The first part of the test requires any restriction on freedom of expression to be provided for by a law which is accessible and "formulated with sufficient precision to enable the citizen to regulate his conduct."[11] Second, the restriction must aim to protect an interest of sufficient importance to warrant overriding a fundamental right. The list of interests in Article 19(3) of the ICCPR is exclusive in the sense that no other interests are considered to be legitimate as grounds for restricting freedom of expression. Third, the restriction must be necessary to secure the interest. The word "necessary" means that there must be a "pressing social need" for the restriction. The reasons given by the State to justify the restriction must be "relevant and sufficient" and the restriction must be proportionate to the aim pursued.[12]

2.2 Specific Internet Standards

2.2.1 It is not contested that the right to freedom of expression applies to the Internet as it does to any other means of communication. Article 19 of the ICCPR, although drafted before the Internet was operational, protects the right to seek, receive and impart information regardless of frontiers and through any media. Specifically addressing freedom of expression and the Internet, the special international mandates on freedom of expression appointed by the United Nations, the Organization for Security and Cooperation in Europe and the Organization of American States adopted a Declaration in 2001 stating:

---

9 See, for example, *Mukong v. Cameroon*, 21 July 1994, Communication No. 458/1991, para. 9.7 (UN Human Rights Committee).

10 *Thorgeirson v. Iceland*, 25 June 1992, Application No. 13778/88, para. 63.

11 *The Sunday Times v. United Kingdom*, 26 April 1979, Application No. 6538/74, para. 49 (European Court of Human Rights).

12 *Lingens v. Austria*, 8 July 1986, Application No. 9815/82, paras. 39-40 (European Court of Human Rights).

The right to freedom of expression applies to the Internet, just as it does to other communication media.[13]

2.2.2 The annual resolutions on Freedom of Opinion and Expression by the UN Human Rights Council include numerous references to the importance of on-line expression, stressing its role in giving effect to freedom of expression. The most recent such resolution recognised, among other things,

the importance of all forms of the media, including the printed media, radio, television and the Internet, in the exercise, promotion and protection of the right to freedom of opinion and expression.[14]

The World Summit on the Information Society, which brought together a range of civil society activists, academics, technical experts, officials and politicians to discuss digital communications technologies, confirmed that the application of traditional human rights standards to on-line expression was "an essential foundation of the Information Society".[15]

2.2.3 Several authoritative international statements go beyond these general statements and prescribe specific rules regarding regulation of the Internet. Perhaps the most detailed and authoritative, since it is a binding international treaty, is the Convention on Cybercrime, adopted by the Council of Europe.[16] The Convention requires States Parties to establish various computer crimes, such as illegal access to a computer system, intercepting or interfering with data, misuse of devices, forgery and fraud, child pornography and breach of copyright.[17] It also requires States Parties to put in place certain procedures and powers to empower authorities to investigate and address computer crimes[18], although it requires these to incorporate adequate safeguards against abuse contrary to human rights.[19]

2.2.4 Several authoritative statements on how to ensure an appropriate balance in the area of Internet regulation between freedom of expression and protecting other social interests have been adopted by the Council of Europe[20] and the special international mandates on freedom of expression.[21]

---

13 Challenges to freedom of expression in the new century: joint statement by the United Nations Special Rapporteur on Freedom of Opinion and Expression, the OSCE Representative on Freedom of the Media and the OAS Special Rapporteur on Freedom of Expression, 20 November 2001, UN Doc. E/CN.4/2002/75, 30 January 2002, Annex V.

14 Resolution 12/16 of the Human Rights Council, adopted on 2 October 2009, UN Doc. A/HRC/Res/12/16.

15 Declaration of Principles, Document WSIS-03/GENEVA/DOC/4-E, 12 December 2003, para.4: http://www.itu.int/wsis/docs/geneva/official/dop.html.

16 Adopted 23 November 2001, E.T.S. No. 185, in force 1 July 2004. Some observers have criticized the Convention for allowing undue restrictions on freedom of expression.

17 See Articles 2-10.

18 See Articles 14-21.

19 Article 15.

20 The leading Council of Europe statement is the Declaration on freedom of communication on the Internet, adopted 28 May 2003. But the Council of Europe has also adopted numerous other statements on specific Internet issues such as protection of children, Internet filters and the right of reply. All of these statements can be found at: http://www.coe.int/t/dghl/standardsetting/media/Doc/CM_en.asp.

21 These include their 2001 Joint Declaration, note 13, their 2005 Joint Declaration, adopted 21 December 2005, and a Joint Declaration by the OSCE Representative and Reporters sans Frontières on

These address issues such as content regulation and the responsibility of Internet service providers (ISPs).

2.2.5 In terms of content regulation, the Council of Europe Declaration on freedom of communication on the Internet states, as its very first Principle:

> *Member States should not subject content on the Internet to restrictions which go further than those applied to other means of content delivery.*

Principle 2 calls for the encouragement of self-regulation or co-regulation in relation to Internet content. And Principle 3 rules out blocking or filtering measures imposed by the authorities, aside from filtering systems to protect children in public access points, for example in schools and libraries, until the competent judicial authorities have come to a provisional or final ruling in the case.

2.2.6 The 2001 Joint Declaration of the special mandates states, bluntly: "States should not adopt separate rules limiting Internet content". The 2005 Joint Declaration elaborates on this, stating:

> *Filtering systems which are not end-user controlled – whether imposed by a government or commercial service provider – are a form of prior-censorship and cannot be justified.*

The same Declaration also states:

> *Restrictions on Internet content, whether they apply to the dissemination or to the receipt of information, should only be imposed in strict conformity with the guarantee of freedom of expression, taking into account the special nature of the Internet.*

2.2.7 These statements also address the question of ISP liability for Internet content. Principle 6 of the Council of Europe Declaration states clearly that service providers should not be expected to monitor Internet content or to actively seek out illegal activity. Providers who simply transmit or provide access to information should not be liable for that content, although where they store content liability might ensue, but only where this was in conformity with the right to freedom of expression.

2.2.8 Once again, the special mandates take a clear position on this issue, stating, in their 2005 Joint Declaration:

> *No one should be liable for content on the Internet of which they are not the author, unless they have either adopted that content as their own or refused to obey a court order to remove that content.*

Guaranteeing Media Freedom on the Internet, adopted on 18 June 2005.

The Joint Declaration by the OSCE Representative and Reporters sans Frontières on Guaranteeing Media Freedom on the Internet is similarly clear, stating, in point 4:

> *A technical service provider must not be held responsible for the mere conduit or hosting of content unless the hosting provider refuses to obey a court ruling. A decision on whether a website is legal or illegal can only be taken by a judge, not by a service provider. Such proceedings should guarantee transparency, accountability and the right to appeal.*

2.2.9 Even before international bodies issued statements on intermediary liability, some countries had started to address the question of who can be held liable for harmful or illegal content through their national laws. In the United States, service providers are explicitly exempted from liability in suits concerning speech by Section 230 of the Communications Decency Act which states:

> *No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.*[22]

This exemption does not extend to Federal criminal law and intellectual property disputes. However, a special 'safe harbour' regime – the Digital Millennium Copyright Act – protects service providers from liability in intellectual property suits.[23]

2.2.10 Article 14 of the 2000 European Commission eCommerce Directive provides immunity to service providers hosting illegal material, provided that they have no actual knowledge of the content in question and quickly remove the content if the service provider is made aware of it. In contrast to US law, the EC Directive only provides for immunity where providers are unaware of the material, whereas the US protection applies even after they become aware of it, a very important distinction. Furthermore, the EC Directive does not extend immunity to search engines and portals that provide links to content. However, many EU countries have extended immunity to such service providers. The EU regime covers both civil and criminal matters.

2.2.11 The Center for Democracy and Technology, looking at different national and regional regimes, suggests that there is a general trend to the effect that governments which seek to maximise growth of the Internet have tended to limit the civil and criminal liability of intermediaries. In contrast, governments in Internet-restrictive countries often hold intermediaries responsible for illegal content posted by users, thus forcing them to become content gatekeepers and hindering innovation.[24]

---

[22] See 47 U.S.C. 230(c)(1)

[23] For a good overview of the DMCA see FAQ (and Answers) about DMCA Safe Harbour www.chillingeffects.org/dmca512/faq.cgi.

[24] See Intermediary Liability: Protecting Internet Platforms for Expression and Innovation, Center for Democracy and Technology, April 2010.

3. Overview of the Thai Computer Crime Act

3.1 The Computer Crime Act, which came into force on 18 July 2007, is currently the key legislation used by Thai authorities to limit the free flow of information on the Internet. It is perhaps significant that the Act was the first bill affecting freedom of expression passed by the National Legislative Assembly installed by the military after the September 2006 coup that toppled the government of former Prime Minister Thaksin Shinawatra.

3.2 Before the enactment of the Act, Thai authorities did not have any specific legal tool 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. Some of these offences could be prosecuted under Thailand's Penal Code, but the Computer Crime Act establishes more specific charges and, in some cases, heavier penalties. Importantly, the Act also gives the authorities the power to block or shut down websites they deem unlawful, a power which they have never before been granted by law.

3.3 Offences in the Act can be grouped into two categories: offences committed against computer systems or computer data (Sections 5-13), and content offences committed via a computer, which are already crimes in the Penal Code (Sections 14-17). It is the second category that has created most of the controversy, as the authorities have applied these provisions to block thousands of websites and to prosecute Internet users and ISPs.

4. Conventional Computer Crimes

4.1 Sections 5 to 13 of the Computer Crime Act establish as criminal offences, punishable by imprisonment of between six months and 20 years and/or a fine of between 10,000 baht (approximately US$300) and 300,000 baht (approximately US$9,036), a variety of crimes against computer systems or computer data. These offences are comparable to the crimes prescribed by the Council of Europe's Convention on Cybercrime and are therefore not as controversial as the latter part of the Act.

4.2 Sections 5 and 6 deal specifically with illegal access to computer systems. Section 5 provides for imprisonment for up to six months and/or a fine of up to 10,000 baht (approximately US$300) for illegally accessing a computer system. Section 6 provides for double the maximum jail term and the maximum fine for illegally disclosing an access code for a computer system in a manner that is likely to cause damage to a third party.[25]

4.3 Sections 7 and 8 deal with illegal access to computer data. Section 7 provides for imprisonment for up to two years and/or a fine of up to 40,000 baht (approximately US$1,204) for illegally accessing computer data. Section 8 raises the penalty to a maximum imprisonment of three years and/or a maximum fine of 60,000 baht (approximately US$1,807) for illegally eavesdropping by electronic means on computer data not intended for use by the general public.[26]

4.4 Sections 9 and 10 deal with illegally damaging computer data or a computer system. Section 9 provides for imprisonment for up to five years and/or a fine of 100,000 baht (approximately US$3,012) for illegally damaging, destroying, amending, altering or adding to a third party's computer data. Section 10 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 normally.[27]

4.5 Section 11 deals with spam. It provides for a fine of up to 100,000 baht (approximately US$3,012), but not for imprisonment, for sending computer data or emails to another person by concealing or forging the source of the data or emails, in a manner that interferes with the use of that computer system by the other person.[28]

4.6 Section 12 provides for much heavier potential penalties where Section 9 or 10 offences cause damage to a large number of people. Section 12 provides for imprisonment for up to 10 years and a fine of up to 200,000 baht (approximately US$6,024) for section 9 or 10 offences where they cause immediate or subsequent damage to the public. The penalty is raised to imprisonment for up to 15 years and a fine of up to 300,000 baht (approximately US$9,036) where the offences are likely to cause damage to computer data or computer systems

[25] These roughly correspond to Articles 2 and 6(1)(a) of the Convention on Cybercrime.
[26] The Convention on Cybercrime does not include specific parallels to these crimes but they are probably largely included within its Article 2 offence.
[27] These roughly correspond to Articles 4 and 5 of the Convention on Cybercrime.
[28] See Article 5 of the Convention on Cybercrime.

related to national security, public security, economic security or public services, or they represent an act against computer data or a computer system available for public use. If these offences cause death, the maximum imprisonment is raised to 20 years.

4.7 Finally, Section 13 deals with distributing computer programmes for the purpose of committing an offence under Sections 5-11. It provides for imprisonment for up to one year and/or a fine of up to 20,000 baht (approximately US$600) for selling or disseminating any set of instructions developed specifically as a tool for committing any crime under those provisions.[29]

[29] Along the lines of Article 6(1)(a) of the Convention on Cybercrime.

5. Controversial Provisions Under Computer Crime Act

5.1 Lèse Majesté

5.1.1 The second set of crimes in the Computer Crime Act, in Sections 14-17, deal with offences which are already a crime under Thailand's Penal Code, but where they are committed by using a computer. There are only four sections in this part of the Act, but as they refer to provisions in the Penal Code, they cover a large variety of offences. The most controversial is Section 14, which includes offences against national security, and hence covers lèse majesté. Lèse majesté has been the single offence most frequently applied by the Thai authorities against Internet users and ISPs under the Computer Crime Act, due in part to the recent political situation in the country (see below). Other sections cover defamation and ISP liability.

5.1.2 Section 14 of the Computer Crime Act provides for imprisonment for up to five years and/or a fine of up to 100,000 baht (approximately US$3,012) for a variety of offences, including importing into a computer system forged or false data in a manner likely to cause damage to a third party or the public (sub-section 1), false data in a manner likely to damage national security or to cause public panic (sub-section 2), data constituting an offence against national security under the Penal Code (sub-section 3) or pornographic data (sub-section 4), or disseminating these types of data.

5.1.3 Section 14 is the main provision Thai authorities have used to charge persons writing or posting material deemed to be defamatory of Thailand's King Bhumibol Adulyadej or the royal family. This has probably made the Computer Crime Act the single most controversial piece of legislation affecting freedom of expression since its enforcement in July 2007.

5.1.4 Lèse majesté is not directly referred to in Section 14, but charges may be laid under sub-sections (2) or (3) since lèse majesté is classified under the heading of Offences Relating to the Security of the Kingdom in the Penal Code. As a result, any law that includes a reference to offences against national security implicitly includes the offence of lèse majesté.

5.1.5 Lèse majesté has been part of the Penal Code since its promulgation in 1957, and it has rarely been amended. Section 112 of the Penal Code, the main provision governing lèse majesté, states: "Whoever defames, insults or threatens the king, the queen, the heir-apparent or the regent shall be punished with imprisonment of three to fifteen years." This is supported by Section 8 of the current 2007 Constitution, which states: "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."

5.1.6 When laying charges for defaming the monarch through the Internet, the police will cite Section 14 of the Computer Crime Act in connection with Section 112 of the Penal Code, as the offence is comprised of provisions of both pieces of legislation. In sentencing a defendant who has been found guilty of committing lèse majesté on the Internet, the court will apply Section

112 of the Penal Code rather than Section 14 of the Computer Crime Act, since the former provides for up to 15 years imprisonment as compared to only five years in the latter.

5.1.7 The crime of lèse majesté has become a matter of domestic and international concern as Thai politics has been polarised around the issue of loyalty to the monarchy since the military coup in September 2006. Anti-royalists are generally considered to support former Prime Minister Thaksin, in exile since the coup, who has been accused by critics of trying to launch campaigns from overseas to destabilise the current government led by the Democrat Party.

5.1.8 In terms of international standards and better practice by other States, Section 14 is problematical. The matter of banning pornography on the Internet has been controversial in other countries, in part because the particular nature of the medium makes it hard to aim protective measures only at children. In a leading 1997 case from the United States, the Supreme Court struck down portions of the Communications Decency Act (CDA), the main purpose of which had been to restrict access by minors to offensive sexual material available over the Internet. The Act was ruled unconstitutional in part because it restricted expression on the entire Internet to the level that would be appropriate for children.[30] The CDA failed to distinguish between the Internet and other forms of expression. Whereas restrictions can be imposed on the time and manner of transmission, or the place of publication, for the broadcast or print media, this is not possible with the Internet.[31]

5.1.9 False news provisions, of the sort found in Section 14, have also been struck down by leading courts in a number of countries. For example, the Supreme Court of Zimbabwe held that a provision which made it a crime to disseminate a statement likely to cause fear, alarm or despondency among the public, or to disturb the peace, was not legitimate as a restriction on freedom of expression[32]. Finally, it may be noted that few democracies, even those with monarchies, have in place lèse majesté laws.

5.2 Internet Service Providers

5.2.1 Section 15 of the Computer Crime Act allows the authorities to charge any ISP who intentionally supports or consents to the commission of an offence under Section 14. The inclusion of the term 'intentionally' protects ISPs who are not aware of the material on their systems. However, once ISPs are informed that the content might be illegal, this defence no longer applies. If found guilty, the ISP faces a penalty equal to that imposed on the offender.

---

30 *Reno v. ACLU*, 521 US 844 (1997).

31 *Ibid.*, pp. 17-21.

32 *Chavunduka & Choto v. Minister of Home Affairs & Attorney General*, 22 May 2000, Judgement No. S.C. 36/2000, Civil Application No. 156/99. See also *R. v. Zundel* [1992] 2 SCR 731 (Supreme Court of Canada).

5.2.2 Some commentators note that there are different kinds of service providers. Some simply provide technical access to the Internet, without hosting or even having access to the content used by their clients. These ISPs, it is argued, should not be responsible for any offence committed by their clients. It may be noted that the Council of Europe's Declaration on freedom of communication on the Internet highlights precisely this point. However, the Computer Crime Act does not recognise different types of service providers. Some commentators also argue that ISPs should not be subject to the same penalty as the primary offenders, as they only provided technical services and did not create the illegal content.

5.2.3 Thai authorities have applied Section 15 to charge ISPs whose websites or systems are alleged to have hosted materials which are prohibited by Section 14. A case in point is the prosecution against prachatai.com, an alternative news website that was accused of hosting statements, posted by a reader, which were offensive to members of the royal family (see section 6.2 for details of this case).

5.2.4 The problem with making ISPs liable for material, even if it is hosted on their servers, is that anyone will be able to censor the Internet, simply by making a claim that the material is illegal, regardless of the merits of that claim. ISPs, wishing to avoid any risk of liability, will simply take it down. For this reason, ISPs are protected by law in several countries.[33]

5.3 Defamation

5.3.1 Defamation is a criminal offence under the Penal Code, carrying a maximum jail term of two years. It has primarily been used to charge print newspapers, but Section 16 of the Computer Crime Act would now allow prosecutions for defamation on the Internet as well.

5.3.2 Section 16 makes it a crime, punishable by up to three years' imprisonment and/or a fine of up to 60,000 baht (approximately US$1,807), to make publicly accessible via a computer system a picture of a third party in a manner that is likely to "impair that third party's reputation or cause that third party to be isolated, disgusted or embarrassed".

5.3.3 Section 16 deals only with defamation by visual means, so it is assumed that defamation on the Internet by means of written text would already be covered by the defamation provisions in the Penal Code. These rules have been in place for a long time and have been widely applied by those who want to sue the print media. The Penal Code also makes it a crime to defame through the broadcast media, whether television or radio.

5.3.4 In sentencing a defendant who has been found guilty of posting defamatory material on the Internet, it is likely that the court will apply the higher jail term of three years provided for in the Computer Crime Act, rather

[33] Section 230 of the US Communications Decency Act protects ISPs in the United State against many forms of liability, although this does not apply to child pornography or to copyright-related matters. Section 5(3) of the German Information and Communications Services Act also provides some protection to ISPs.

than the lower term of two years in the Penal Code. This may be contrasted with the crime of lèse majesté, for which the penalties in the Penal Code are much harsher. A number of website operators have been charged with defamation under the Computer Crime Act, but none of these cases have yet been finally decided by the courts.

5.3.5 In most countries, images are by definition not defamatory, since they involve neither false statements of fact nor unwarranted opinions, although they may have been taken in breach of a privacy right. Otherwise, in most established democracies, the general rules on defamation apply to defamatory statements on the Internet.[34] Furthermore, it is increasingly being realised that criminal defamation cannot be justified as a restriction on freedom of expression, and more-and-more States are doing away entirely with their criminal defamation laws, and relying instead on the civil law to protect reputations.[35]

[34] Possibly with some amendment in relation to where a case for this may be lodged.
[35] The United Kingdom, for example, abolished its criminal defamation laws in October 2009.

6. Vast Powers Bestowed on the Authorities

6.1 The Computer Crime Act grants the authorities vast powers to investigate and gather evidence of an offence committed by or via computer. Section 18 allows the competent officials, among other things, to copy computer data or computer traffic data from any computer system suspected of being used for an offence, to access any computer data or computer system for the purpose of gathering evidence, to decode any person's computer data, and to seize or attach any computer system for up to 90 days, for purposes of investigation and evidence gathering.

6.2 The powers under Section 18 are set out in eight sub-sections, but the Act does not indicate how the competent officials should apply them. As a result, officials have the discretion to choose which procedure they wish to use, regardless of the impact this might have on the suspect. Officials, for example, can choose to seize an entire computer system or data storage device, rather than simply copying the data they want and returning the computer. Some observers have argued that the Act should only allow officials to take the least intrusive action which will support their investigation, taking into consideration factors such as personal data the suspect might have on the computer and the effect on his or her livelihood.

6.3 Where information is deemed to affect national security, which includes lèse majesté, or to be contrary to public order or good morals, which includes pornography, Section 20 allows the authorities, with the approval of the Minister of Information and Communication Technology, to seek a court warrant to restrain the dissemination of the information directly, or ask an ISP to do it for them. This leaves the decision of whether to bring an action before a court to block or close down websites, web boards or blogs entirely up to the discretion of officials. Some people have argued that a special committee, whose membership includes representatives of ISPs, media lawyers and Internet users, should make such decisions, which should still be subject to approval by court order.

6.4 Since the Act first came into force, the Ministry of Information and Communication Technology has applied Section 20 to shut down or block thousands of websites or web pages alleged to contain lèse majesté or pornographic materials. The Minister has made the crackdown a policy priority. In January 2009, the Senate did the same, setting up a committee to address the issue, and indicating that over 10,000 websites could be targeted by the campaign. Freedom Against Censorship Thailand (FACT), a Bangkok-based network set up to promote freedom of expression on the Internet, publishes a list of these blocked websites on its website, www.facthai.wordpress.com.

6.5 Exercising these Sections 18 and 20 powers requires a court warrant. However, Thai courts are very often cooperative in granting warrants in cases involving allegations of lèse majesté. Furthermore, Section 18 allows officials to exercise certain powers – such as obtaining mandatory oral or written testimony, other documents or computer traffic data from ISPs – without a court warrant. Some have argued that officials should be required to obtain a court warrant for the exercise of any power under these sections.

7. Cases Prosecuted Under Computer Crime Act

7.1 Suwicha Thakhor – An Oil Rig Mechanic

7.1.1 As noted above, the vast majority of the cases brought so far under the Computer Crime Act have been for lèse majesté, due in part to the current political polarisation in Thailand. All of the accused have been citizens who were not involved in politics and who used the Internet to express and share their views on the monarchy.

7.1.2 In the middle of January 2009, while shopping with his wife at a marketplace in his hometown in the north-eastern town of Nakhon Phanom, Suwicha Thakhor, a mechanic in his mid-30s who was working for a foreign oil rig, was arrested by the police for posting defamatory materials about King Bhumibol Aduyadej on YouTube. He was charged with two counts of breach of the law for postings made on 15-16 August 2008 and 26 December 2008-15 January 2009. He was denied bail and has been kept in jail since his arrest.

7.1.3 Suwicha made a confession during the police investigation and then pleaded guilty during the trial, in part because the police had convinced him that if he did not fight the case he would receive a less severe penalty and would stand a better chance of receiving a royal pardon. On 3 April 2009, the criminal court in Bangkok, applying the higher penalty under the Penal Code, sentenced him to 10 years each for the two counts, but reduced to five years each due to his guilty plea. He is now serving his 10-year term, hoping for a royal pardon.

7.1.4 Suwicha is the first person to be convicted under the Computer Crime Act, and his case generated both domestic and international media coverage. International organisations campaigning for freedom of expression have voiced concerns that Suwicha's acts were a legitimate exercise of his rights, and, furthermore, that his punishment was disproportionate, and have called for his early release.

7.2 Prachatai.com – A Forum for Free Expression

7.2.1 Prachatai.com was first launched in 2004 as an alternative news website, presenting news and articles on issues rarely covered by the established media. It also offers web boards for readers to post their opinions without prior screening of the content. The popularity of prachatai.com has soared among urban and educated Thais since the September 2006 coup, in terms of both visits and postings.

7.2.2 Prachatai.com says its policy is to comply with the law, particularly the Computer Crime Act, in relation to its news website and web boards. It has been warned by authorities about certain lèse majesté content, but said it complies with such warnings by taking the content down.

7.2.3 On 6 March 2009, police officers from the Crime Suppression Division in Bangkok came to prachatai.com's office to arrest its director, Chiranuch Premchaiporn, charging her under Sections 14 and 15 of the Computer Crime Act. The police claim lèse majesté statements were posted for 20 days on prachatai.com from 15 October to 3 November 2008.

7.2.4 Before arresting Chiranuch, the police interrogated prachatai.com staff on a few occasions regarding other material posted on its web boards. In late 2008, the police obtained the Internet protocol (IP) of one of the persons who posted the statements from prachatai.com (this is computer data that prachatai.com is required to retain under the law). The police have arrested and charged this individual, whose case is now pending before the courts.

7.2.5 On 31 March 2010, State prosecutors decided to file Chiranuch's case with the criminal court in Bangkok, which has set 31 May 2010 as the date for her first court appearance. Chiranuch is facing 10 counts of offences of violating Section 15 of the Computer Crime Act, for 10 different alleged postings of material on the prachatai.com website, allegedly in breach of the rule on lèse majesté, which together carry a maximum sentence of 50 years' imprisonment. Chiranuch, however, is not being charged under the Penal Code, pursuant to which she would face an even higher possible penalty.

7.3 Individuals Involved with Fall of the Stock Market

7.3.1 In the middle of October 2009, Thai stock prices plunged for two successive days, following rumours posted on the Internet that King Bhumibol's health had deteriorated after he was hospitalised in mid-September. The King has since made several public appearances on various occasions. As of late April 2010, he remains in hospital.

7.3.2 In November 2009, Thai authorities charged four individuals under Section 14 of the Computer Crime Act for posting the rumours on the Internet, on the basis that they imported false data into a computer system which was likely to damage national security or to cause a public panic. All the accused have been released on bail and their cases have not yet been filed with the court.

8. Proposed Changes to the Computer Crime Act

8.1 The Computer Crime Act has been in force for only two and a half years, but efforts are already underway to amend it. The Senate's Committee on Science, Technology, Information and Telecommunication has set up a working group to make reform proposals. The working group – whose members include website operators, ISPs, bloggers and lawyers – has proposed extensive changes to the controversial Sections 14 and 16 of the Act.

8.2 The working group has recommended repealing all of the current Section 14 offences and replacing them with only two offences. These are using a computer system to deceive other people in order to gain computer data or assets and importing child pornography into a computer system. The group is recommending that all mention of national security be dropped from Section 14.

8.3 The working group has also proposed that defamation under Section 16 would only cover the posting of indecent material. The group has also proposed making it a crime to violate intellectual property rights.

8.4 The working group is not proposing any change to the provisions involving offences against computer systems or computer data – the so-called conventional computer crimes (Sections 5-13) – and it is only proposing minor changes to the authority of competent officials under the Act. The group's proposals would also retain the rules on liability of ISPs.

8.5 The amendments proposed by the working group are still being considered and it is likely to take some time before they are presented to parliament for its consideration. Officials at the Ministry of Information and Communication Technology, which is responsible for the execution of the Computer Crime Act, indicated in an interview with the authors that that the ministry does not currently plan to propose alternative amendments to the law.