



ARTICLE 19

GLOBAL CAMPAIGN FOR FREE EXPRESSION

Thailand: Draft Computer Offences Act

**A Memorandum on the draft Computer-Related
Offences Commission Act currently
being developed by the Thai authorities.**

London
April 2007

ARTICLE 19 · 6-8 Amwell Street · London EC1R 1UQ · United Kingdom
Tel +44 20 7278 9292 · Fax +44 20 7278 7660 · law@article19.org · <http://www.article19.org>

TABLE OF CONTENTS

1. Introduction	1
2. International Standards	1
2.1 Guarantees of Freedom of Expression.....	1
2.2 Restrictions on Freedom of Expression	2
2.3 Freedom of Expression and the Internet.....	3
3. Analysis of the Draft Act.....	4
3.1 Crimes Established by the Draft Act	4
3.2 The Powers of Competent Officials	10

Summary of Recommendations

Recommendations on Crimes Established:

- The sanctions provided for under the draft Act should be reviewed and tailored more appropriately to the (often not very major) seriousness of the offences.
- Consideration should be given to limiting the rule on eavesdropping in section 8 to situations where the context shows the data being sent was intended for a limited audience.
- Consideration should be given either to removing section 9, referring to illegally damaging data, entirely from the law or at least to amending it so that it is limited to situations which are appropriate for criminal measures.
- Consideration should be given to removing section 11, providing for harsher sanctions for breach of section 9 and/or 10, altogether from the law. Alternatively, it should be restricted to situations in which there was an intention to damage important and clearly defined interests such as a threat to the integrity or security of the country.
- Section 12, making it a crime to sell 'sets of instructions' used to commit the crimes established by sections 5-10 should be substantially narrowed so that it applies only to the intentional sale of instructions that are specifically designed to perpetrate those crimes.
- Section 13, providing restrictions on the acquisition of various types of data, should be removed from the law in its entirety.
- Section 14, requiring service providers to delete data acquired in breach of section 13, should be removed from the law in its entirety.
- Section 15, establishing an offence of harm to reputation, should be removed from the law in its entirety.
- Section 19, permitting competent officials to ban sets of instructions, very broadly defined, should be restricted in scope to instructions which can be used to undermine the legitimate use of computer systems.

Recommendations on Powers of Competent Officials:

- There should be judicial oversight for the exercise of any powers that intrude on the right to privacy or the right to freedom of expression.
- A judicial warrant should be required for access to any computer data or system.
- Warrants should be granted only when other measures to obtain the information have failed, or are not likely to provide information of the evidentiary value required, and when proposed surveillance or seizure of data or equipment is proportionate to the purpose.
- Limitations should be placed on the duration of judicial warrants.

1. Introduction

This Memorandum sets out ARTICLE 19's observations on the draft Computer-Related Offences Commission Act (draft Act) currently being prepared by the Thai authorities.¹ We understand that the draft Act has already passed the first reading and is currently being reviewed by a 25-member panel before being presented for a second reading. The primary aim of the draft Act, as reflected in the title, is to address the problem of computer-related crime. This is a legitimate and, indeed, important social objective. At the same time, some of the provisions in the draft Act trench on the right to freedom of expression. This Memorandum seeks to highlight our concerns with the current draft Act.

The comments in this Memorandum are based on established international law and international best practice in the area of freedom of expression, as well as specific standards relating to the Internet. The Memorandum is intended as input to the process of drafting this law, with the goal of helping to ensure that the final product is consistent with international and constitutional guarantees of freedom of expression. It contains our analysis of the existing provisions in the draft Act, along with recommendations for reform.

For the most part, the draft Act seeks to provide protection against acts analogous to wrongs that have already been recognised in the criminal law. However, given that its provisions, for the most part, affect freedom of expression, particular care needs to be taken in establishing these wrongs. Many are unduly vague or go beyond what is necessary to protect legitimate interests. Sections 13 and 15, which make it a crime to access certain types of information over the Internet, are of particular concern. We are also concerned at the broad-ranging powers of surveillance and access to communications systems granted to 'competent officials', which violate privacy rights and exert a real chilling effect on the right to freedom of expression. The following pages first set out international standards on freedom of expression, and then elaborate our concerns regarding the draft Act.

2. International Standards

2.1 Guarantees of Freedom of Expression

Article 19 of the *Universal Declaration on Human Rights* (UDHR)² guarantees the right to freedom of expression in the following terms:

Everyone has the right to freedom of opinion and expression; this right includes the right to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.

The UDHR, as a UN General Assembly resolution, is not directly binding on States. However, parts of it, including Article 19, are widely regarded as having acquired legal force as customary international law since its adoption in 1948.³

¹ Our analysis is based on an unofficial translation of the draft Act provided to us in February 2007. We take no responsibility for errors based on translation.

² UN General Assembly Resolution 217A(III), adopted 10 December 1948.

³ For judicial opinions on human rights guarantees in customary international law, see, for example, *Barcelona*

ARTICLE 19

GLOBAL CAMPAIGN FOR FREE EXPRESSION

The *International Covenant on Civil and Political Rights* (ICCPR),⁴ a treaty which has been ratified by over 150 States, including Thailand,⁵ imposes formal legal obligations on State Parties to respect its provisions and elaborates on many of the rights included in the UDHR. Article 19 of the ICCPR guarantees the right to freedom of expression in terms very similar to those found at Article 19 of the UDHR:

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.

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*,⁶ Article 10 of the *European Convention on Human Rights*⁷ and Article 13 of the *American Convention on Human Rights*.⁸ The right to freedom of expression enjoys a prominent status in each of these regional conventions and, although these are not directly binding on Thailand, judgments and decisions issued by courts under these regional mechanisms offer an authoritative interpretation of freedom of expression principles in various different contexts.

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."⁹ As the UN Human Rights Committee has said:

The right to freedom of expression is of paramount importance in any democratic society.¹⁰

2.2 Restrictions on Freedom of Expression

The right to freedom of expression is not absolute. Both international law and most national constitutions recognise that freedom of expression may be restricted. However, any limitations must remain within strictly defined parameters. Article 19(3) of the ICCPR lays down the conditions which any restriction on freedom of expression must meet:

Traction, Light and Power Company Limited Case (Belgium v. Spain) (Second Phase), ICJ Rep. 1970 3 (International Court of Justice); *Namibia Opinion*, ICJ Rep. 1971 16, Separate Opinion, Judge Ammoun (International Court of Justice); *Filartiga v. Pena-Irala*, 630 F. 2d 876 (1980) (US Circuit Court of Appeals, 2nd Circuit). Generally, see M.S.McDougal, H.D.Lasswell, L.C.Chen, *Human Rights and World Public Order*, Yale University Press (1980), pp. 273-74, 325-27.

⁴ UN General Assembly Resolution 2200A(XXI), adopted 16 December 1966, in force 23 March 1976.

⁵ Thailand ratified the ICCPR in January 1997.

⁶ Adopted 26 June 1981, OAU Doc. CAB/LEG/67/3 rev. 5, 21 I.L.M. 58 (1982), in force 21 October 1986.

⁷ Adopted 4 November 1950, E.T.S. No. 5, in force 3 September 1953.

⁸ Adopted 22 November 1969, O.A.S. Treaty Series No. 36, 1144 U.N.T.S. 123, in force 18 July 1978.

⁹ 14 December 1946. This Resolution refers to freedom of information in its broad sense, as the free circulation of information and ideas.

¹⁰ *Tae-Hoon Park v. Republic of Korea*, 20 October 1998, Communication No. 628/1995, para. 10.3.

ARTICLE 19

GLOBAL CAMPAIGN FOR FREE EXPRESSION

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 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.¹¹ 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.¹²

First, the interference must be provided for by law. This requirement will be fulfilled only where the law is accessible and “formulated with sufficient precision to enable the citizen to regulate his conduct.”¹³ Second, the interference must pursue a legitimate aim. The list of aims in the various international treaties are exclusive in the sense that no other aims are considered to be legitimate as grounds for restricting freedom of expression. Third, the restriction must be necessary to secure one of those aims. 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.¹⁴

2.3 Freedom of Expression and the Internet

It is beyond doubt that the right to freedom of expression applies to the Internet as it does to any other means of communication. Article 19 of the Universal Declaration on Human Rights, although drafted some twenty years before the Internet was first conceived of, protects the right to seek, receive and impart information *through any media and regardless of frontiers* (emphasis added).

Specifically addressing freedom of expression and the Internet, the UN, OSCE and OAS Special Mandates on freedom of expression adopted a Declaration in 2001 stating that:

The right to freedom of expression applies to the Internet, just as it does to other communication media.¹⁵

¹¹ See, for example, *Mukong v. Cameroon*, 21 July 1994, Communication No. 458/1991, para. 9.7 (UN Human Rights Committee).

¹² *Thorgeirson v. Iceland*, 25 June 1992, Application No. 13778/88, para. 63.

¹³ *The Sunday Times v. United Kingdom*, 26 April 1979, Application No. 6538/74, para. 49 (European Court of Human Rights).

¹⁴ *Lingens v. Austria*, 8 July 1986, Application No. 9815/82, paras. 39-40 (European Court of Human Rights).

¹⁵ 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.

ARTICLE 19

GLOBAL CAMPAIGN FOR FREE EXPRESSION

This statement was welcomed by the UN Commission on Human Rights, whose 2002 and 2003 resolutions on freedom of expression include numerous references to the importance of on-line expression, stressing its importance as a means of expression and encouraging access to it.¹⁶ Similar statements have been made by the Committee of Ministers of the Council of Europe,¹⁷ the African Commission on Human and Peoples' Rights¹⁸ and the Representative on Freedom of the Media of the Organisation for Security and Cooperation in Europe.¹⁹ The World Summit on the Information Society, a gathering of government leaders to discuss issues related to electronic communications, confirmed the applicability of traditional human rights standards on-line "as an essential foundation of the Information Society".²⁰

3. Analysis of the Draft Act

3.1 Crimes Established by the Draft Act

The draft Act establishes a number of criminal offences for various acts in relation to computers and information stored on computers. For the most part, these are accepted wrongs in many countries and, in many cases, they are based on analogous wrongs committed outside of the context of computers. At the same time, ARTICLE 19 has a number of concerns with the crimes established by the draft Act.

Sanctions

As a preliminary comment, we note that for many offences the sanctions envisaged, which in all cases include imprisonment, are excessive, in some cases almost absurdly so; in one case even including capital punishment. Eavesdropping, for example, can lead to imprisonment for up to three years, amending computer data five years, and doing so in a way that causes bodily damage, life imprisonment or capital punishment. This latter punishment is presumably discordant with the sanctions found in the Thai Penal Code relating to (potentially minor) bodily harm, which we assume envisages this extreme punishment only for the very most serious criminal offences.

We recognise that there is considerable latitude in the application of penalties, and that in most cases the penalties provided are maximums, but in some cases the draft Act stipulates minimum periods of imprisonment for crimes. This is probably contrary to the right not to be arbitrarily deprived of liberty and it also makes no sense. For example, a combination of section 10, prohibiting the disruption of a computer system, and section 11(2), increasing the penalty where the act is perpetrated against a computer available for public use, would lead to a minimum imprisonment term of three years for someone who, as a poor practical joke, pulled the plug on a computer in library, causing his friend to lose the document they

¹⁶ Commission on Human Rights Resolution 2003/42, 23 April 2003, E/CN.4/2003/L.11/Add.4; Commission on Human Rights resolution 2002/48, 23 April 2002, E/CN.4/2002/200.

¹⁷ See its Declaration on freedom of communication on the Internet, adopted 28 May 2003.

¹⁸ See its Declaration of Principles on Freedom of Expression in Africa, adopted at its 32nd Session, 17 - 23 October 2002.

¹⁹ See Freedom of the Media and the Internet, Amsterdam Recommendations, 14 June 2003.

²⁰ 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>.

were working on. Even wilfully damaging a public computer system, for example through vandalism, would rarely merit such a severe sanction.

We believe that these sanctions are disproportionate and cannot be justified. Article 9 of the ICCPR, which protects the right to liberty, requires any deprivation of liberty to be proportionate. This means that, at minimum, the minimum term envisaged in various provisions of the draft Act should be dropped.

In addition, it should be noted that in cases involving a form of expression, the imposition of a sanction – whether monetary or through deprivation of liberty – engages the right to freedom of expression. This restricts the level of a fine that may be imposed, or the length of any imprisonment. Under international law, it is well established that excessive sanctions, even for otherwise legitimate restrictions, represent a breach of the right to freedom of expression. The European Court of Human Rights, for example, has noted that excessive sanctions exert an unacceptable chilling effect on freedom of expression. In *Tolstoy Miloslavsky v. the United Kingdom*, it ruled that excessive damages for defamation violated Article 10 of the Convention: “[U]nder the Convention, an award of damages for defamation must bear a reasonable relationship of proportionality to the injury to reputation suffered”.²¹ In that case, even though sanctions for a particularly egregious defamation were warranted, the damages awarded of £1.5 million were excessive and, since they did not meet the proportionality test, they unjustifiably restricted freedom of expression.²²

Section 8

Section 8 provides protection for computer users against ‘eavesdropping’, unless it was “intended for the public interest or general people’s use”. This is clearly a provision designed to protect the privacy and confidentiality of computer usage, and hence one that promotes freedom of expression. At the same time, the override provision quoted above is unduly vague and leaves significant scope to ‘competent officials’ to apply this rule subjectively. We believe that every person has a legitimate expectation of privacy in electronic communications, as is reflected in the first part of Section 8, and are concerned that the override would weaken that expectation in unpredictable and possibly unjustifiable ways. We therefore recommend that it be removed. We are similarly concerned at the limitation of the prohibition to data that is “in process of being sent”; this may be too limited to provide any real protection to computer users.

We also recommend that a definition of “eavesdropping” is provided, and that it includes keylogging as well as other ways of accessing data.

Section 9

Section 9 makes it a crime ‘illegally’ to damage, destroy, correct, change or amend a third party’s computer data, subject to a maximum imprisonment of five years and/or a fine of up to 100,000 bhat. It is not entirely clear to us what this provision means but we assume for purposes of this analysis that the term ‘illegal’ implies reference to another law which already makes the act a legal wrong. If so, we are not aware of the existing provisions to which this section refers, and so cannot comment on them. Presumably they are all intended

²¹ 13 July 1995, Application No. 18139/91, para. 49.

²² *Ibid.*, para. 51.

ARTICLE 19

GLOBAL CAMPAIGN FOR FREE EXPRESSION

to provide protection to the third party's use of his or her computer system and, to that extent, protect freedom of expression.

At the same time, we note that, if the referenced wrong is criminal in nature, the import of section 9 is presumably limited to the penalty. It is unclear why the draft Act should alter a penalty already provided for under another law. If the referenced wrong is civil in nature, providing for compensation, it is unclear why the draft Act should seek to add a criminal penalty to this. While a number of wrongs exist in both the civil and criminal laws, this is mostly the case where a recognised crime, such as assault or theft, may also cause personal loss and the aim is to provide for the possibility of compensation for that loss. Care must be taken when converting what was originally a civil wrong into a criminal wrong, to observe the strictures of the criminal law.

Section 11

This section provides for enhanced penalties for acts in breach of sections 9-10 where these either: a) cause damage (section 11(1)); or b) are likely to damage data or a computer system "related to the country's security, public security and economic security or public services or is an act against computer data or a computer system available for public use" (section 11(2)). The problem with the very extreme severity of the crimes provided for under this section has already been noted.

Section 11(1) makes little sense in relation to many of the crimes established by sections 9-10, given that they already explicitly or implicitly incorporate the notion of damage. In these cases, section 11(1) provides for enhanced penalties for the same wrong.

Some of the interests listed under section 11(2), namely economic security and public services, are unacceptably broad as restrictions on freedom of expression. Vague notions like these can easily be abused to sanction a wide range of activities. Others, such as acts against public computer data or systems, do not warrant higher penalties than acts against private computer systems, which already run to five years' imprisonment.

The remaining interests, namely the country's security and public security, although important interests, are potentially extremely broad in nature. Given the very serious penalties these crimes attract, these terms should be defined clearly and narrowly. Finally, the term 'related to' is extremely unclear. It is one thing, and a potentially serious offence, to damage data with the purpose and effect of harming security and quite another, and a much less serious offence, to damage data which simply happens to relate to security.

Section 12

Section 12 makes it a crime to sell or distribute "sets of instructions developed as a tool used in committing an offence" under sections 5-10. This section is extremely problematical for a number of reasons. First, it is quite unclear what it would apply to. It may be noted that a vast array of software may potentially be put to bad use: virus writers, for example, use normal programming software to write viruses and may use entirely legitimate encryption tools to communicate with each other. To spread their viruses, they use normal internet protocols and perfectly legitimate peer to peer software. To render all of this illegal would clearly be inappropriate. Second, the position of innocent disseminators such as ISP needs to be taken into account: they should not be rendered liable if one of their users uploads virus writing software to their site. Similarly, retailers of computer tools

ARTICLE 19

GLOBAL CAMPAIGN FOR FREE EXPRESSION

would not want to sell anything that might breach this provision and, as a result, may stop selling an unduly wide range of products. Third, assuming its primary focus is to prevent the dissemination of tools which are designed specifically to perpetrate the crimes established by sections 5-10 (assuming for the sake of argument that such tools indeed exist), the focus of this provision should be on the maker or designer of those tools rather than the disseminator, although we do recognise that they may often be beyond Thailand's jurisdictional reach.

Section 13

Section 13 establishes a number of vague and, at least in translation, confusing prohibitions on accessing a computer system to:

- acquire data so as to cause a third party to believe that the data belongs to or has been prepared by another party, in a manner likely to cause damage to either the third party or the public (section 13(1));
- to acquire false computer data in a manner likely to damage the country's security or to cause public panic (section 13(2));
- to acquire data 'related with' a criminal code offence against security, and "being publicly accessible" (section 13(3)); and
- to acquire data "of a pornographic nature that is publicly accessible" (section 13(4)).

Pursuant to section 13(5), dissemination or re-sending data known to be covered by any of the preceding provisions attracts a penalty of up to five years' imprisonment and/or up to 100,000 bhat.²³ Acquiring pornographic data involving persons of less than 18 years old will result in imprisonment of two to five years and/or a fine of between 40,000 and 100,000 bhat.

It may be noted that, inasmuch as these provisions apply to the acquisition of information, they trench directly on the right to freedom of expression. Like section 12, section 13 is very problematical from a freedom of expression perspective. It is hard to see what general interest is being protected by section 13(1). It might include, for example, cases of fraud or other pre-recognised wrongs, but these are by definition already provided for in law. It is not justifiable to restrict freedom of expression unless it is for the benefit of a clear public or private interest falling within the scope of the restrictions listed in Article 19(3). The vague reference to damage to the third party or the public is not enough to establish an overriding interest which would warrant a restriction on this right.

Similarly, section 13(2) does not appear to protect any legitimate interest. It may be noted that false information is clearly protected by the guarantee of freedom of expression and laws prohibiting the dissemination of such information with similarly vague references to public panic have been held to be unconstitutional in Zimbabwe and Canada.²⁴ The reasoning in those cases focused on the subjective nature of the notion of falsity, the chilling effect of false news provisions, the lack of any sufficient interest being protected and the possibility of abuse. It is, furthermore, hard to understand what particular threat might be caused to national security by false information obtained via a computer system,

²³ We note that, at least in our English translation, no separate penalty is prescribed for breach of sections 13(1)-(4). We assume that this is a mistake.

²⁴ See *Chavunduka & Choto v. Minister of Home Affairs & Attorney General*, 22 May 2000, Judgement No. S.C. 36/2000, Civil Application No. 156/99 (Supreme Court of Zimbabwe) and *R. v. Keegstra* [1990] 2 SCR 697 (Supreme Court of Canada).

ARTICLE 19

GLOBAL CAMPAIGN FOR FREE EXPRESSION

over and above pre-existing threats which the general criminal law of Thailand presumably already protects against.

Section 13(3), at least as it appears in English translation, seems to be quite illegitimate. Information which is publicly available is, almost by definition, not a threat to national security. Even if information contains material which is damaging to national security, where it is already public, at best very limited further harm results from further publication, which should not, as a result, be restricted. A case before the European Court of Human Rights involved claims by the United Kingdom that a book containing the memoirs of a former spy was harmful to national security. The book had already been published in the United States and copies were widely available in the United Kingdom. The Court held that further publication of the book would not increase the harm already caused to national security and that, as a result, prohibiting such publication was illegitimate. This provision also suffers from the lack of clarity associated with the term ‘related with’, as noted above.

It is not clear whether or not the term ‘pornographic material’ as used in section 13(4) refers to a definition already established by Thai law. If so, it is unclear why that section is necessary since the existing provisions presumably already make it illegal to possess pornographic material obtained over the Internet. If not, this section is illegitimate as a restriction on freedom of expression, since the term ‘pornography’ is not defined in the draft Act and is therefore unacceptably vague. The same reasoning applies to the more serious punishments associated with pornography involving persons under 18 years of age.

Section 14

Section 14 extends liability for a breach of section 13 to service providers who are aware of the breach but fail immediately to delete the information. Given that we recommend the removal of section 13 from the law, we obviously also recommend that section 14 be removed. Regardless of the approach adopted vis-à-vis section 13, however, we still recommend that section 14 be removed. Service providers are not an appropriate locus of responsibility for determining whether or not material under their control falls foul of the section 13 prohibitions. Faced with any potential risk of liability, they will naturally and understandably err on the side of caution, removing any material they consider might possibly breach the section 13 prohibitions. It is obvious that this will lead to a seriously overbroad application of those prohibitions, to the detriment of freedom of expression.

Section 15

This section, the motivation for which is, frankly, extremely difficult to understand, makes it a crime to alter a picture of a third party in a way likely to harm that third party’s reputation or to cause him or her to be “isolated, disgusted or embarrassed”. Where the maligned third party has died, his or her parents, spouse or children may bring an action.

Thai law already has developed both civil and criminal defamation provisions designed to protect reputation. It is both illegitimate and unnecessary to add to these, since they already provide ample, and in some cases excessive, protection for reputation, including using computers.²⁵ Furthermore, ARTICLE 19 believes that criminal defamation laws,

²⁵ See ARTICLE 19’s November 2004 Memorandum on the Thai defamation laws, available on our website at: www.article19.org.

ARTICLE 19

GLOBAL CAMPAIGN FOR FREE EXPRESSION

particularly where they envisage imprisonment as a sanction, breach the right to freedom of expression.

There are also serious problems with this provision on its own merits. It is bizarre that it focuses only on a third party's picture from among the potentially vast array of defamatory material that might be available online. Simply accessing a picture can engage liability, even where no measure has been taken to disseminate the picture to another person. This flies in the face of defamation laws the world over, which require an imputation to be made to another person which lowers the reputation of the plaintiff. It is sufficient if the picture is likely to lower the third party's reputation, or even to embarrass that third party. Once again, this is vastly broader than the rules found in defamation laws around the world which, in striking a delicate balance between freedom of expression and protection of reputation, require actual harm to reputation, not just the likelihood thereof. Protecting a third party from embarrassment, furthermore, is not a sufficiently important interest to warrant overriding the fundamental right to freedom of expression. Unlike other defamation laws, including Thai defamation laws, there are no defences. Thai criminal law, for example, provides for a good faith in the protection of a legitimate interest defence. Finally, the draft Act allows for proceedings to be brought on behalf of a deceased person. ARTICLE 19 considers it to be illegitimate to protect the reputation of a deceased person, although certain other claims on their behalf, such as for loss of material benefits, might be legitimate.

Section 19

This section allows a competent official to restrict the use, possession or dissemination of 'undesirable sets of instructions', defined very broadly to include, among other things, instructions which correct or change a computer system. Broadly speaking, there are two problems with this to impose serious permanent restrictions on the use of computers. We believe that this power ought to be reserved to the courts, and that officials should have this power only when necessary to prevent imminent danger to life or limb. Second, as defined, practically any software could be covered by this. We recommend that this provision should instead be limited to sets of instructions that can be used to harm the legitimate use of computers.

We are also concerned at section 25, which allows competent officials to impose 'administrative' fines of up to 200,000 bhat, and daily fines of up to 5,000 bhat, on individuals who obstruct them in the performance of their duties under Section 19. These are extensive powers which should be allocated to courts, perhaps outside of situations where urgent action is required to prevent serious harm being caused. While non-judicial officials have the power to impose minor administrative fines, such as parking tickets, in all jurisdictions, the powers under the draft Act go far beyond that.

Recommendations:

- The sanctions provided for under the draft Act should be reviewed and tailored more appropriately to the (often not very major) seriousness of the offences.
- Consideration should be given to providing a legal definition of 'eavesdropping' and removing the limitations currently stated in section 8.
- Consideration should be given either to removing section 9 entirely from the

ARTICLE 19

GLOBAL CAMPAIGN FOR FREE EXPRESSION

law or to amending it so that it is limited to situations which are appropriate for criminal measures.

- Consideration should be given to removing section 11 altogether from the law. Alternatively, section 11(1) should be removed, the interests in section 11(2) should either be removed or defined clearly and narrowly, and it should be clarified that the section applies only to actions intended to damage the protected interests.
- Section 12 should be substantially narrowed so that it applies only to the intentional sale of ‘sets of instructions’ that are specifically designed to perpetrate the crimes established by sections 5-10.
- Section 13 should be removed from the law in its entirety.
- Section 14 should be removed from the law in its entirety.
- Section 15 should be removed from the law in its entirety.
- Section 19 should be restricted in scope to sets of instructions which can be used to undermine the legitimate use of computer systems. Competent officials should be able to use the powers under section 19 only where this is necessary to prevent imminent and serious harm.
- The powers granted to ‘competent officials’ in section 25 should be transferred to the courts.

3.2 The Powers of Competent Officials

The main powers of competent officials are set out in section 16 of the draft Act. These effectively grant such officials very broad powers to copy data from computers, to demand that such data be provided to them, to inspect computer systems and/or to seize equipment, whenever they have reasonable cause to believe that an offence has been committed under the Act. Some restrictions are imposed on the use of these powers. In exercising two of the eight significantly overlapping powers, officials need to report their reasons to a court within 24 hours (see section 18). A letter of seizure must be issued before equipment may be seized, and such action is limited to 30 days although this may be extended for up to another 60 days by a court (section 17). Some limitations are also imposed on the disclosure of data acquired under section 16 to others (sections 20-23).

The powers granted to competent officials under section 16 are in many ways analogous to the interception of telecommunications messages, while in other ways they are more analogous to search and seizure powers. It is apparent that the use of both kinds of powers exerts a chilling effect on the right to freedom of expression. The UN Special Rapporteur on Freedom of Expression has therefore stated that, “in the interception of communications a fair balance and proportionality should be maintained.”²⁶ The use of these powers also interferes with the right to privacy, which is protected under Article 17 of the ICCPR, and which must be justified by reference to criteria similar to those described in Section 2.2 of this Memorandum. This means that the powers should be used only when truly necessary, in a manner that is proportionate, and that safeguards need to be in place to prevent their abuse.

²⁶ Report of the Special Rapporteur, Visit to the United Kingdom of Great Britain and Northern Ireland, UN Doc. E/CN.4/2000/63/Add.3, 11 February 2000, para. 73.

ARTICLE 19

GLOBAL CAMPAIGN FOR FREE EXPRESSION

There exists a wealth of caselaw and national practice, from international institutions as well as from national jurisdictions, on which safeguards are needed to maintain the ‘fair balance and proportionality’ referred to by the Special Rapporteur.²⁷ First, it follows from both Articles 17 and 19 of the ICCPR that all surveillance operations require a clear basis in law, and the laws concerned must be readily accessible and sufficiently precise so that citizens will be aware of the circumstances in which they apply.²⁸ The European Court of Human Rights, which has considered a number of cases concerning surveillance of communications, has stressed that: “It is essential to have clear, detailed rules on the subject, especially as the technology available for use is continually becoming more sophisticated.”²⁹

Second, measures such as data surveillance or the seizure of equipment must be used only when truly ‘necessary’ – “[an] adjective [that is] not synonymous with ‘indispensable’, neither has it the flexibility of such expressions as ‘admissible’, ‘ordinary’, ‘reasonable’, or ‘desirable’”.³⁰ Measures taken should also be proportionate, meaning that they should be strictly limited to that what is required to achieve the legitimate objective.

Third, there must be safeguards built into the legislative framework to prevent abuse of surveillance powers.³¹ A system of judicial oversight is an essential safeguard to prevent abuse and has been put in place in many countries. For example, in the United States a court order is required to gain access to data such as emails.³²

None of the above safeguards are present in the draft Act. Section 16 allows a wide range of persons to access computer data if they have any reasonable cause to believe an offence has been committed, subject to only very limited ex post facto judicial supervision. There is no requirement of true necessity or of proportionality, or any requirement that the proposed power of access should be used as a measure of last resort only. We urge that this be remedied by putting in place a system of strong judicial oversight for the exercise of any powers that intrude on the right to privacy or the right to freedom of expression. In particular, a judicial warrant should be required for access to any computer system, be it to access the content of files or communications, or to communications data such as a log of files visited or emails sent. Limitations should be placed on the duration of such warrants, and on the use that may be made of material obtained pursuant to the warrant. Additionally, the law should require the use of intrusive powers only as a last resort, and in a manner that is proportionate to the aim of the measure.

Recommendations:

²⁷ For an overview of international best practice and caselaw as well as recommendations on how to design a ‘fair’ surveillance system, see JUSTICE, *Under Surveillance: Covert Policing and Human Rights Standards*, London 1998 (<http://www.justice.org.uk>). Further comparative material may be found in a consultation paper by the Irish Law Reform Commission, *Privacy: Surveillance and Interception*, Dublin: 1996.

²⁸ *Malone v. the United Kingdom*, 2 August 1984, Application No. 8691/79 (European Court of Human Rights), para. 67.

²⁹ *Kruslin v. France*, 24 April 1990, Application No. 11801/85 (European Court of Human Rights), para. 33.

³⁰ *Handyside v. the United Kingdom*, 7 December 1976, Application No. 5493/72 (European Court of Human Rights), at para. 48.

³¹ *Klass and others v. Federal Republic of Germany*, 6 September 1978, Application No. 5029/71 (European Court of Human Rights), para. 50.

³² Electronic Communications Privacy Act of 1986, 18 U.S.C. § 2510.

ARTICLE 19

GLOBAL CAMPAIGN FOR FREE EXPRESSION

- There should be judicial oversight for the exercise of any powers that intrude on the right to privacy or the right to freedom of expression.
- A judicial warrant should be required for access to any computer data or system.
- Warrants should be granted only when other measures to obtain the information have failed, or are not likely to provide information of the evidentiary value required, and when proposed surveillance or seizure of data or equipment is proportionate to the purpose.
- Limitations should be placed on the duration of judicial warrants.

ANNEX: The Draft Act in English Translation

Office of the Council of State
April 2005

The draft law already read by the OCS
Supplementary Issue No. 257/2548

Memorandum of the Principles and Reasons
Supporting the Computer-Related Offence Commission Bill

Principles

There shall be a law governing the perpetration of computer-related offences.

Reasons

Today a computer system is essential to business operations and the human way of life, as such, if any person commits an act that disables the working of a computer system according to the pre-determined instructions or that causes a working error – a deviation from that required by the pre-determined instructions or that resorts to any means to illegally know of, correct or destroy a third party's data contained in a computer system or that uses a computer system to disseminate false or pornographic computer data, then that act will damage and affect the country's economy, society and security including people's peace and good morals. Therefore, it is deemed appropriate to stipulate measures aimed at preventing and suppressing such acts. Hence the enactment of this Act.

The Computer-Related Offences Commission Bill B.E...

As it is deemed appropriate to enact a law governing the commission of a computer-related offence.

This Act contains certain provisions governing the restrictions of an individual's rights and freedom permissible by Section 29, together with Sections 31, 37, 39, 48 and 50 of the Kingdom of Thailand's Constitution by virtue of legal provisions.

ARTICLE 19
GLOBAL CAMPAIGN FOR FREE EXPRESSION

Section 1 This Act shall be called the “Computer-Related Offences Commission Act B.E.....”.

Section 2 This Act shall be enforceable from the day following the date of its publication in the Government Gazette.

Section 3 In this Act,

“Computer System” means a piece of equipment or sets of equipment units, whose function is integrated together, for which sets of instructions and working principles enable it or them to perform the duty of processing data automatically.

“Computer Data” means data, statements or sets of instructions contained in a computer system, the output of which may be processed by a computer system

“Computer Traffic Data” means data related to computer system-based communications showing sources of origin, starting points, destinations, routes, time, dates, volumes, time periods, types of services or others related to that computer system’s communications.

“Service Provider” shall mean:

(1) A person who provides service to the public with respect to access to the Internet or other mutual communication via a computer system, whether on their own behalf, or in the name of, or for the benefit of, another person

(2) A person who provides services with respect to the storage of computer data for the benefit of the person under (1) “Service User” means a person who uses the services provided by a service provider, with or without fee

“Competent Official” means a person appointed by a Minister to perform duties under this Act.

“Minister” means a Minister who has responsibility and control for the execution of this Act.

Section 4. The Minister of Information and Communications Technology shall have responsibility and control for the execution of this Act and shall have the authority to issue a Ministerial Rule for the purpose of the execution of this Act

A Ministerial Rule shall be enforceable upon its publication in the Government Gazette.

Chapter 1

Computer-Related Offences

Section 5. Any person accessing a computer system for which a specific access prevention measure that is not intended for their use is available shall be subject to imprisonment for no longer than one month or a fine of not more than one thousand baht or both; the offence under paragraph one shall be a compoundable offence.

ARTICLE 19

GLOBAL CAMPAIGN FOR FREE EXPRESSION

Section 6. If any person knowing of a measure to prevent access to a computer system specifically created by a third party discloses that measure in a manner that is likely to cause damage to the third party, then they shall be subject to imprisonment for no longer than six months or a fine of not more than ten thousand baht or both.

Section 7. If any person accesses computer data, for which there is a specific access prevention measure not intended for their own use available, then he or she shall be subject to imprisonment for no longer than one year or a fine of not more than twenty thousand baht or both; the offence under paragraph one shall be a compoundable offence.

Section 8. Any person who commits any act by electronic means to eavesdrop a third party's computer data in process of being sent in a computer system and not intended for the public interest or general people's use shall be subject to imprisonment for no longer than three years or a fine of not more than sixty thousand baht or both.

The provisions under paragraph one shall not apply to the eavesdropping of computer data according to a computer data owner's specific instructions.

Section 9. Any person who illegally damages, destroys, corrects, changes or amends a third party's computer data, either in whole or in part, shall be subject to imprisonment for no longer than five years or a fine of not more than one hundred thousand baht or both; the offence under paragraph one shall be a compoundable offence.

Section 10. Any person who commits any act that causes the working of a third party's computer system to be suspended, delayed, hindered or disrupted to the extent that the computer system fails to operate normally shall be subject to imprisonment for no longer than five years or a fine of not more than one hundred thousand baht or both.

Section 11. The perpetration of an offence under Section 9 or Section 10 that:

(1) causes damage, whether it be immediate or subsequent and whether it be synchronous to the public's computer data shall be subject to imprisonment for one to ten years or a fine of twenty thousand to two hundred thousand baht or more, or both;

(2) is an act that is likely to damage computer data or a computer system related to the country's security, public security and economic security or public services or is an act against computer data or a computer system available for public use shall be subject to imprisonment from three years up to fifteen years and a fine of sixty thousand baht up to three hundred thousand baht.

The commission of an offence under (2) that causes damage to people's body or life shall be subject to capital punishment, life-time imprisonment or imprisonment from ten years up to twenty years.

Section 12. Any person who sells or disseminates sets of instructions developed as a tool used in committing an offence under Section 5, Section 6, Section 7, Section 8, Section 9 or Section 10 shall be subject to imprisonment for no greater than one year or a fine of not greater than twenty thousand baht, or both.

Section 13. If any person commits any of the following acts:

(1) that involves access to a computer system for acquiring computer data in a manner that causes a third party to believe that that computer data belongs to a third party or is prepared by a third party in a manner that is likely to cause damage to that third party or the public;

ARTICLE 19

GLOBAL CAMPAIGN FOR FREE EXPRESSION

(2) that involves access to a computer system for acquiring false computer data in a manner that is likely to damage the country's security or to cause a public panic;

(3) that involves access to a computer system for acquiring any computer data related with an offence against the Kingdom's security under the Criminal Code and being publicly accessible;

(4) that involves access to a computer system for acquiring any computer data of a pornographic nature that is publicly accessible;

(5) that involves the dissemination or re-sending of computer data already known to be computer data under (1) (2) (3) or (4), in which case imprisonment for no longer than five years or a fine of not more than one hundred thousand baht, or both shall be imposed

If pornographic computer data under (4) displays a picture of a person aged less than eighteen years old, imprisonment from two years up to five years or a fine of forty thousand up to one hundred thousand baht, or both shall be imposed.

Section 14. Any service provider knowing of the perpetrating of an offence under Section 13 within a computer system under their control but failing to delete immediately the computer data contained therein shall be subject to the same penalty as that imposed upon a person committing an offence under Section 13.

Section 15. Any person, who accesses a computer system, to acquire computer data in which there appears a third party's picture created, edited, added or adapted by electronic means or otherwise in a manner that is likely to impair that third party's reputation or causes that third party to be isolated, disgusted or embarrassed, shall be subject to imprisonment for no longer than three years or a fine of not more than sixty thousand baht, or both.

An offence under paragraph one shall be a compoundable offence.

If a party injured by an offence under paragraph one has died before filing a complaint, then their parents, spouse or children may file a complaint and shall be deemed to be the injured party.

Chapter 2

Competent Officials

Section 16. If there is reasonable cause to believe that there is the perpetration of an offence under this Act, then a relevant competent official shall have the following authority to:

(1) instruct a person who possesses or controls computer data or computer data storage equipment to deliver to the relevant competent official the computer data or the equipment pieces necessary to identify the person who has committed an offence;

(2) copy computer data from a computer system, in which there is a reasonable cause to believe that offences under this Act have been committed;

(3) inspect or access a computer system, computer data, computer traffic data or computer data storage equipment belonging to any person that is evidence of, or may be used as evidence related to, the commission of an offence or used in identifying a person who has committed an offence, and if necessary, instruct that person to send the relevant computer data to all necessary extent as well;

ARTICLE 19

GLOBAL CAMPAIGN FOR FREE EXPRESSION

(4) decode any person's computer data or instruct any person related to the encryption of computer data to decode the computer data or cooperate with a relevant competent official in decoding;

(5) call for computer traffic data related to communications from a service user via a computer system or from other relevant persons, exclusive of the contents of the data mutually communicated between persons;

(6) instruct a service provider to deliver to a relevant competent official service users-related data that must be stored under Section 24 or that is in the possession or under the control of a service provider;

(7) seize or attach the suspect computer system for the purpose of obtaining details of an offence and the person who has committed an offence under this Act;

(8) issue an inquiry letter to any person related to the commission of an offence under this Act or summon them to give statements, forward written explanations or any other documents, data or evidence in an understandable form.

Section 17. Regarding the seizure or the attachment under Section 16 (3), a relevant competent official must issue a letter of seizure or attachment to the person who owns or possesses that computer system as evidence. This is provided, however, that the seizure or attachment shall not last for longer than thirty days. If the seizure or the attachment requires a longer time period, a petition shall be filed with a criminal court for the extension of the seizure or attachment time period. However, the court may allow a single or several time extensions, however altogether for no longer than sixty days. When that seizure or attachment is no longer necessary or upon its expiry date, a competent official must immediately return the computer system that was seized or withdraw the attachment.

The letter of seizure or attachment under paragraph one shall be in accordance with a Ministerial Rule.

Section 18. A relevant competent official shall exercise the authority under Section 16 only to the necessary extent for the purpose of preventing and suppressing an offence under this Act. The copying of computer data under Section 16 (2) shall be done only when there is a reasonable ground to believe that an offence under Section 9 has been committed and in a manner that does not present an unnecessary obstacle to the operation of a business by the person who owns or possesses the computer data.

When a relevant competent official has acted as under Section 16 (3) or (5), the details concerning actions to be taken and the reasons behind such actions must be recorded and then be reported to a provincial court with jurisdiction or a criminal court within twenty-four hours from the starting time of the action. If the court deems that that any action is contradictory to paragraph one or paragraph two, the court shall order that the action be suspended.

Section 19. If a relevant competent official found that any computer data contains undesirable sets of instructions, a relevant competent official with the authority to prohibit the sale or dissemination of such, may instruct the person who owns or possesses the computer data to suspend the use of, destroy or correct the computer data therein, or to impose a condition with respect to the use, possession or dissemination of the undesirable sets of instructions.

ARTICLE 19

GLOBAL CAMPAIGN FOR FREE EXPRESSION

The undesirable sets of instructions under paragraph one shall mean to include sets of instructions that cause computer data, a computer system or other instruction sets to be damaged, destroyed, corrected, changed, added, interrupted or, fail to perform according to pre-determined instructions or otherwise as required by a relevant Ministerial Rule, with the exception of sets of instructions aimed at preventing or correcting the foregoing sets of instructions as required by a Minister and published in the Government Gazette.

Section 20. A relevant competent official shall not disclose or deliver computer data, computer traffic data or service users' data acquired under Section 16 to any person.

The provisions under paragraph one shall not apply to any actions performed for the benefit of lodging a lawsuit against a person who has committed an offence under this Act or for the benefit of lodging a lawsuit against a relevant competent official on the grounds of their abuse of authority or for action taken according to a court's trial-related instruction.

In the case where a law empowers a person to summon documentary evidence or data or summon any person to give statements for the purposes of legal proceedings and that such is not the case under paragraph two, that law shall not apply to the data acquired by a relevant competent official under Section 16 and delivered to the competent official, as the case may be.

Any competent official who violates paragraph one must be subject to imprisonment for no longer than two years or a fine of not more than forty thousand baht, or both.

Section 21. Any competent official who commits an act of negligence that causes a third party to know of computer data, computer traffic data or a service user's data acquired under Section 16 must be subject to imprisonment for no longer than one year or a fine of not more than twenty thousand baht, or both.

Section 22. Any person knowing of computer data, computer traffic data or a service user's data acquired by a relevant competent official under Section 16 and disclosing it to a third party shall be subject to imprisonment for no longer than two years or a fine of not more than forty thousand baht, or both.

Section 23. Computer data, computer traffic data or a service user's data acquired through the perpetration of an offence under Section 20 or Section 21 or Section 23 shall not be admissible as evidence for taking any action that is harmful to the person who owns or possesses the data

Section 24. A service provider must store computer traffic data for at least thirty days from the date on which the data is input into a computer system. However, if necessary, a relevant competent official may instruct a service provider to store data for a period of longer than thirty days but not exceeding ninety days on a special case by case basis or on a temporary basis.

If a service provider enters into an agreement to provide service to a service user, the service provider shall retain details of the agreement for a period of at least thirty days after the date on which the agreement expires.

The types of service provider to whom the provisions under paragraph one shall apply and the timing of this application shall be established by a Minister and published in the Government Gazette.

A service provider who fails to comply with this Section must be subject to a fine of not greater than five hundred thousand baht.

ARTICLE 19

GLOBAL CAMPAIGN FOR FREE EXPRESSION

Section 25. If any person obstructs the performance of duties by a relevant competent official or fails to comply with the instructions of a relevant competent official under Section 16 or Section 19 or fails to comply with the conditions imposed by a relevant competent official under Section 19, then a relevant competent official granted such power shall instruct that person to pay an administrative fine of not more than two hundred thousand baht and a further daily fine of not more than five thousand baht until the relevant corrective action has been taken.

If the person instructed to pay the administrative fine under paragraph one does not pay the fine, then the provisions governing administrative enforcement under the law governing administrative state service-related procedures shall apply *mutatis mutandis*.

When the person who is instructed to pay the fine has paid the administrative fine, the right over a criminal lawsuit shall be extinguished.

Section 26. Regarding the appointment of a competent official under this Act, a Minister shall appoint such person from among state officers with a knowledge of, and expertise in, computer systems and who has undergone the training course required by a Minister.

Section 27. In the performance of duties, a relevant competent official must produce an identity card to a relevant person.

The identity card shall be as per the form required by a Minister and published in the Government Gazette.

Section 28 In performing the duties under this Act, the competent official required by a Minister shall be an administrative officer or senior police officer under the Criminal Procedure Code.

In arresting, controlling, searching, investigating, and filing a lawsuit against a person who commits an offence under this Act, and for what is within the authority of an administrative officer or a police officer, or an administrative officer or a senior police officer, or an inquiry officer under the Criminal Procedure Code, the administrative officer or the police officer, the administrative officer or the senior police officer or the inquiry officer shall take action only upon the request of a relevant competent official under this Act. The Prime Minister is in charge of the Royal Thai Police Headquarters and with a Minister shall have a joint authority to establish a regulation with respect to the means and action-related procedures under paragraph two.

Countersigned

.....

Prime Minister