Singapore Journal of Legal Studies
[1998] 260 – 298

SECTION 5 OF THE OFFICIAL SECRETS ACT, *BRIDGES* AND BEYOND

The recent cases on the Official Secrets Act have, to a certain extent, clarified and limited the scope of criminal liability under section 5 of the Act. This article examines the local decisions and contrasts them with Malaysian and English developments on the subject. Some suggestions for further improvement in this area of the law are made.

THE Official Secrets Act[1] ("the Act") was first introduced to Singapore more than sixty years ago as the Official Secrets Ordinance, 1935.[2] The purpose of the Act is stated in the long title as "to prevent the disclosure of official documents and information". This is achieved, *inter alia*, *via* section 5 which imposes criminal penalties for activities described by the marginal note as "wrongful communication, *etc*, of information".

Section 5 of our Act is modelled closely on section 2 of the Official Secrets Act 1911 in the UK,[3] which has been criticised for its width and incomprehensibility. The 1972 Departmental Committee Report on Section 2 of the Official Secrets Act 1911 described the UK provision as "obscurely drafted, and to this day legal doubts remain on some important points of interpretation"[4] and that "people are not sure what it means, or how it operates in practice, or what kinds of action involve real risk of prosecution under it".[5] According to one calculation, over 2,000 differently worded charges can be brought under it.[6] Another report is even more direct in its criticism:

1 Cap 213, 1985 Rev Ed.

2 Ordinance No 25 of 1935.

3 For an account of the history and operation of the UK Act, see David Williams, *Not in the Public Interest* (1965); David Hooper, *Official Secrets* (1987). S 2 (UK) Official Secrets Act 1911 has since been repealed and replaced by the (UK) Official Secrets Act 1989.

4 Report of the Departmental Committee on Section 2 of the Official Secrets Act 1911 (Cmnd 5104, 1972), para 16 [hereinafter referred to as the "Franks Committee Report"].

5 Franks Committee Report, *ibid*, para 88.

6 *Ibid*, para 16.

> The drafting of section 2 is archaic and, in places, obscure. But the central objection is to its scope. It penalises the disclosure of *any* information obtained by a person ... however trivial the information and irrespective of the harm likely to arise form its disclosure. The "catch-all" nature of section 2 has long been criticised. Although in practice prosecutions are not brought for the harmless disclosure of minor information, it is objectionable in principle that the criminal law should extend to such disclosure. The excessive scope of section 2 has also led to its public reputation as an oppressive instrument for the suppression of harmless and legitimate discussion. Because section 2 goes so much wider than what is necessary to safeguard the public interest, its necessary role in inhibiting harmful disclosures is obscured.[7] (Emphasis in the original)

Our recent case law on section 5 of the Act, culminating in the reference to the Court of Appeal questions of law in *PP* v *Bridges Christopher*,[8] will be analysed in this article. Section 5 of the Act is a goldmine to any criminal law practitioner, public prosecutor or academic. Ambiguities abound as to the *mens rea* and *actus reus* elements and the scope of the defences available under the provision. It will be argued that these cases have, to a certain extent, clarified and limited the scope of criminal liability under section 5 of the Act. The next step in the development of this area of the law is in formulating a clear and coherent principle to be applied. When this is achieved, the difficulties encountered in ascertaining the type of information which is protected and the conduct which is subject to criminal sanctions under section 5 of the Act can be easily resolved.

I. Whether all Information is Regulated or Only Information which, by its Nature, is an "Official Secret"

With regard to section 2 of the (UK) Official Secrets Act 1911, it was commonly assumed that the offence applied to all information, irrespective of its nature, importance or source:

7 Reform of Section 2 of the Official Secrets Act 1911 (Cm 408, 1988), para 8 [hereinafter referred to as the "1988 UK White Paper"]. There have been various attempts to reform the UK provision by successive Governments and MPs, see *ibid*, paras 9-12. The criticism of this provision is universal. The Canadian Official Secrets Act, which is also modelled closely on the UK version, had been described by the 1969 Mackenzie Royal Commission on Security as "an unwieldy Statute couched in very broad and ambiguous language", cited in *R* v *Toronto Sun Publishing Limited* (1979) 47 CCC (2d) 535, 543. The court added that "a complete redrafting of the Canadian *Official Secrets Act* seems appropriate and necessary".

8 [1998] 1 SLR 162 (CA).

> The main offence which section 2 creates is the unauthorised communication of official information (including documents) by a Crown servant. The leading characteristic of this offence is its catch-all quality. It catches all official documents and information. It makes no distinctions of kind, and no distinctions of degree. All information which a Crown servant learns in the course of his duty is "official" for the purposes of section 2, whatever its nature, whatever its importance, whatever its original source. A blanket is thrown over everything, nothing escapes.[9]

In *R* v *Crisp and Homewood*,[10] it was held that section 2 of the (UK) Official Secrets Act 1911 applied to any document or information of an official character, and not only such information as would be injurious to the State. The title of the Act, "Official Secrets", was not sufficient to cut down the unambiguous words of the section.

The approach in the UK is supported by the legislative history of the provision. The original section 2 of the (UK) Official Secrets Act 1911 did not have the following words in bold. These were added later by the (UK) Official Secrets Act 1920:

> 2(1) If any person having in his possession or control **any secret official code word, or pass word, or** any sketch, plan, model, article, note, document or information ....
>
> (2) If any person receives any **secret official code word, or pass word, or** sketch, plan, model, article, note, document, or information ....

This addition of words strongly suggested that the words "sketch, plan, model, article, note, document, or information" were not meant to be read restrictively when the provision was originally enacted in 1911. Hence, the words "secret official" only qualified the words "code word or pass word", particularly as they are separated by the word "any" before "sketch" in section 2 (1) of the (UK) Official Secrets Act 1911. Furthermore, it should be noted that the addition of words was brought about by section 10 of

[9] Franks Committee Report, *supra*, note 4, para 17. A later paragraph clarifies that it is not only Crown servants who are governed by the provision, *ibid*, para 19. See also 1988 UK White Paper, *supra*, note 7, para 8.

[10] (1919) 83 JP 121, 122. This was approved in *R* v *Galvin* [1987] 1 QB 862, 869; and in the case of Aubrey, Berry and Campbell, see Andrew Nicol, "Official Secrets and Jury Vetting" [1979] Crim LR 284, 289.

the (UK) Official Secrets Act 1920, which specifically stated that the amendments "relate to minor details". Hence, it would be surprising for the words "secret official" to qualify all subsequent terms in the provision.

However, the discomfort with such wide ranging liability can be seen in the local cases.[11] In *Bridges Christopher*,[12] the learned Chief Justice said that, "[i]t would be quite wrong to interpret a penal provision so widely that innocent persons' liberty depends on the exercise of discretion [by the Attorney General to consent to institute prosecution]".

While Justice Thean, as he then was, in *PP* v *Phua Keng Tong*[13] accepted that the words "secret official" only qualified the words "code word, countersign or password" and not "any photograph, drawing, plan, model, article, note, document or information" in our Act; the learned Chief Justice, in *Bridges Christopher*[14] on the other hand, proceeded on the basis that the information obtained or received in contravention of section 5 of the Act must be "secret official" information.

This conflict in the cases has since been resolved by the Court of Appeal through its answer to the first question of law referred to it in *Bridges Christopher*.[15] The Court of Appeal held that:

> As a matter of construction the collocation of words in section 5(1) of the Act logically fall into two groups: 'any secret official code word, countersign or password' is one group (the first group) and the other

[11] The same uncertainty as to the words qualified by "secret" or "official" also arose in Canada, see the 1969 Mackenzie Royal Commission on Security, paras 204, 206, cited in *Toronto Sun Publishing Limited, supra*, note 7, at 544; Ontario Law Reform Commission, *Report on Political Activity, Public Comment and Disclosure by Crown Employees* (1986) pp 103, 187. The Malaysian Official Secrets Act 1972 (Act 88), which is also modelled on the (UK) Official Secrets Acts of 1911 and 1920, was amended in 1986, *vide* the Official Secrets (Amendment) Act 1986 (Act A A660), to clarify that only "any official secret or any secret official code word, countersign or password" is encompassed in the offence of wrongful communication or receipt of information. At the same time, a definition of "official secret" was added.

[12] [1997] 1 SLR 406, para 24 (HC).

[13] [1986] 2 MLJ 279, 282.

[14] *Supra*, note 12, para 15 (HC). See also *supra*, note 8, para 29 (CA) and *Toronto Sun Publishing Limited, supra*, note 7, at 545 where it was held that, "[s]ecrecy must lie in the very nature of the document itself and in the existing circumstances surrounding and affecting the document".

[15] *Supra*, note 8 (CA): Question 1(a), "Whether the word 'information' in s 5(1) of the OSA, in the context in which it is enacted refers to: (i) 'secret official ... information' as described in paragraphs (a) to (e) of that subsection, or (ii) any information as described in paragraphs (a) to (e) of that subsection ...".

> group is, 'any photograph, drawing, plan, model, article, note, document or information' (the second group). ...[16]
>
> ... the words, 'secret official' qualify or govern only the words in the first group, namely code word, countersign and password and not the words in the second group, namely photograph, drawing, plan, model, article, note, document and information.[17]

However, the items in the second group are only protected if they fall within and are used in one of the ways specified by the sub-paragraphs to section 5(1):

> The sting in the second group of words is not in the words 'secret official' but in paras (a), (b), (c), (d) and (e) .... Taking 'information' as an example ... the question is not whether the information is 'secret official information' but in the context of this case whether the information is 'information obtained in contravention of this Act' (s 5(1)(c)) .... And again in the context of this case the offence is committed when that information is communicated 'to any person other than a person to whom he is authorised to communicate it or to whom it is his duty to communicate it' (sub-para (i) of sub-s (1)). ...[18]
>
> ...in the case of the first group of words – code word, countersign or password – each is qualified or governed by the words 'secret official' and no further qualification is required to make them 'protected' under s 5(1). The offence is committed when the code word, countersign or password is used in any of the ways specified in paras (i) to (iv) of s 5(1).[19]

This interpretation limits the apparently wide ambit of the offence under section 5(1) of the Act.

However, the meaning of the terms "secret official" which qualify the first group of words is still unclear. It is submitted that in order to place all the offences created by section 5 of the Act on par, the words "secret

16 *Ibid*, para 35 (CA).
17 *Ibid*, para 38 (CA).
18 *Ibid*, para 35 (CA). This was also the conclusion reached by Thean J, as he then was, in *Phua Keng Tong, supra*, note 13, at 282. Thean JA was a member of the Court of Appeal in *Bridges Christopher*.
19 *Ibid*, para 37 (CA).

official", which are not defined in the Act, should be given the same meaning as paragraphs (a) to (e). There can be no reason why the situations in which a "code word, countersign or password" are considered protected should be different from a "photograph, drawing, plan, model, article, note, document or information".[20] Any difference in the scope of protection will lead one group of words to become otiose.

Hence, a "code word, countersign, or password" may be considered as "secret official" only if it relates to or is used in a prohibited place or anything in such a place (paragraph (a)); relates to munitions of war (paragraph (b)); has been made or obtained in contravention of the Act (paragraph (c)); has been entrusted in confidence to him by any person holding office under the Government (paragraph (d)); or he has obtained, or to which he has had access, owing to his position as a person who holds or has held office under the Government, or as a person who holds, or has held a contract made on behalf of the Government, or as a person who is or has been employed under a person who holds or has held such an office or contract (paragraph (e)). In short, there are only five types of protected "information" under section 5 of the Act regardless of the form it takes (code word, countersign, password, photograph, drawing, plan, model, article, note, document or information). Any "information" is protected so long as it is within any one of paragraphs (a) to (e).

Secondly, in the interests of consistency, the words "photograph, drawing, plan, model, article, note, document or information" in section 5(2) of the Act should be similarly qualified since it must be "communicated ... in contravention of [the] Act". This is despite the fact that paragraphs (a) to (e) are not repeated under subsection (2).

Thirdly, the approach of the Court of Appeal may also be supported by the application of accepted principles of statutory construction. It is a settled rule for the construction of penal statutes that any ambiguity is resolved in favour of the accused.[21] Furthermore, where the provision impinges on the exercise of a constitutionally protected right, such restrictions must be strictly interpreted.[22] It was expressly recognised in *Phua Keng Tong*[23] that

[20] This argument for consistency will also apply to all instances where the terms "secret official" appear, *eg*, s 3(1)(c) Official Secrets Act (Cap 213, 1985 Rev Ed).

[21] *Teng Lang Khin* v *PP* [1995] 1 SLR 372, following *Tuck & Sons* v *Priester* (1887) 19 QBD 629.

[22] *Ong Ah Chuan* v *PP* [1981] AC 648; *Minister for Home Affairs* v *Fisher* [1980] AC 319.

[23] *Supra*, note 13. Although the Court of Appeal in *Dow Jones Publishing Company (Asia) Inc* v *AG* [1989] 2 MLJ 385 did not decide on the issue, the court assumed that the right of freedom of speech and expression included the right to receive information. It was also

the right to freedom of speech and expression protected under Article 14(1)(a) of the Singapore Constitution encompassed the communication or dissemination of information and that section 5(1) of the Act impinges on this right.[24]

II. "Official" Information

In *PP* v *Lim Kit Siang*,[25] the Malaysian High Court held that:

> It is significant to note that the word "secret" is attached to the word "official" such that they may appropriately be referred to as "official secret". The word "official" seems to signify the nature or character of the secret and it also denotes the category the secret belongs to. In the light of the definition of the word "official" as relating to any public service the words "official secrets" read together must therefore refer to secrets relating to any public service, or public service secrets or Government secrets.

It should be noted that this definition of the term "official" referred to in the Malaysian Official Secrets Act[26] is not found in our Act and, therefore, should not limit the understanding given to the type of information protected under our Act. The scope of modern government means that more information about the private affairs of individuals come into the possession of the Government than ever before. It is too narrow to restrict the type of protected information to that relating to the public service or the Government. Protection should also encompass personal information supplied confidentially by members of the public to the Government, such as information supplied to the Central Provident Fund Board and the Inland Revenue Authority of Singapore.[27]

the opinion of the Indian Supreme Court that the freedom of speech and expression in Art 19(1)(a) Indian Constitution, which is *in pari materia* with Art 14(1)(a) Singapore Constitution (1992 Ed), includes the right to acquire information and to disseminate it, *Secretary, Ministry of Information & Broadcasting* v *Cricket Association of Bengal* (1995) 2 SCC 161, paras 43, 201.

24 It is not suggested that the Act itself may be *ultra vires* since Art 14(2)(a) Singapore Constitution (1992 Ed) allows Parliament to impose restrictions on the freedom of speech and expression which it considers *inter alia* necessary or expedient in the interests of the security of Singapore. See also *Phua Keng Tong* v *PP, supra*, note 13, at 283.

25 [1979] 2 MLJ 37, 40 (HC).

26 S 2 (Malaysian) Official Secrets Act 1972 (Act 88) states that "official" relates to any public service.

27 *Supra*, note 12, paras 18, 27 (HC). See also Franks Committee Report, *supra*, note 4, paras 192, 197. Some of the specific legislation protecting such information are listed at footnote 63, *infra*.

On the other hand, the Act does not protect information which is not of an "official" character. This apparently excludes information which is concerned solely with the affairs of a statutory body or a Government company,[28] which is regulated by other means.[29]

III. Information in the Public Domain

The proposition that information which is already in the public domain, namely by being published or made publicly available,[30] can never be protected under the Act was soundly rejected in both the High Court and Court of Appeal decisions in *Bridges Christopher*.[31] Consideration must be given to how the information reached the public domain. If it is as a result of unauthorised disclosure, that information is still protected.

The Court of Appeal explained that information in the public domain may be divided into two types: (a) where knowledge of the information is universal (for example, "the sun rises in the east"); or (b) where information initially protected by the Act enters the public domain by the authority of the appropriate Government department. Such information is not regulated by section 5 of the Act:

> The former category of information because of its universality belies proof while information in the latter category raises a question of fact to be proved ... the onus of which is on the prosecution.[32]

It is respectfully submitted that the resolution of this public domain argument is far from satisfactory. In the event of a conflict between the two categories of information described above, it is unclear which will

[28] See Prof S Jayakumar's speech on moving the Statutory Bodies and Government Companies (Protection of Secrecy) Bill, *Singapore Parliamentary Debates, Official Reports*, 20 December 1983, col 219.

[29] *Eg*, Statutory Bodies and Government Companies (Protection of Secrecy) Act (Cap 319, 1985 Rev Ed). There is also the civil tort of confidentiality and disciplinary measures for civil servants.

[30] *Supra*, note 12, paras 29, 30 (HC).

[31] *Ibid*, para 19 (HC); *supra*, note 8, para 39 (CA). See also *Boyer* v *The King* (1949) 94 CCC 195, 244 where in relation to the Canadian Official Secrets Act, it was said that "the *Official Secrets Act*, by its very title, indicates that its provisions are not applicable to what is already published or made public and coming within the public domain". However, this approach was rejected in England, see *R* v *Galvin*, *supra*, note 10.

[32] *Supra*, note 8, para 39 (CA). Hence, the Court of Appeal's answer to Question 1(b), "In particular, does information that has been published, released or made available to the public by a person authorised to do so nevertheless remain information falling within s 5 of the OSA?", was in the negative. See also *Bridges Christopher, supra*, note 12, para 40 (HC).

predominate. For example, protected information which is leaked to a journalist who then publishes it. Although the information may not be known universally, it may very well reach a wide cross-section of the general public. Conversely, the mere fact that the information has reached a large number of persons does not necessarily mean that it is in the public domain, such as where the persons who have knowledge of the confidential information are under an obligation not to disclose it without authority.

Furthermore, it is uncertain to what extent the information needs to be disseminated or objectively ascertainable before it will be considered to be "universal". In *Bridges Christopher*,[33] the learned Chief Justice in the High Court accepted that the latest addresses and the dates of the change of addresses could, in principle, be protected information under section 5 of the Act. Hence, such information was not treated as belonging to the "sun rises in the east" category. It is unclear why this is so. One's address can be easily determined without the person's co-operation, for example by watching the person's movements or by making enquiries of the person's friends and relatives.

This approach also places too much emphasis on the public availability of the information and ignores any impact the subsequent publication the information may have. Hence, it has been said that the difficulty of retrieving the particular piece of information already made available to the public does not mean it is protected under the Act.[34] However, there is a converse situation in which a second or subsequent disclosure of information, albeit publicly available, may be more harmful. For example, a newspaper story about a certain matter may carry little weight in the absence of firm evidence of its validity. However, confirmation of the story by a senior official of the Government can be very much more damaging.[35] Another situation is where information has been previously published piecemeal in a number of sources but a subsequent publication may bring it to the attention of people who would otherwise be unlikely to learn of it. For example, the publication of a list of addresses of persons in public life[36] or the defence capabilities of naval craft under tender may capture the interest of terrorist groups much more readily than the same information scattered in disparate

[33] *Supra*, note 12, para 34 (HC).

[34] *Ibid*, paras 38, 65 (HC).

[35] 1988 UK White Paper, *supra*, note 7, para 62.

[36] *Ibid*. The same qualification was made by Lord Keith in *AG* v *Guardian Newspapers (No 2)* [1990] 1 AC 109, 260 in relation to the circumstances in which the duty of confidentiality in the civil law may arise.

previous publications.

It is proposed that instead of focusing on the public availability of the information, the analysis should be on the degree of harm that may follow from a subsequent publication of the information. This "harm analysis" is discussed further below.

IV. Classification by the Government

The Act does not require that the information or document be classified as "secret", "confidential" or "restricted" before it is considered as protected under the Act. In *Phua Keng Tong*,[37] two of the documents with which the first accused was convicted of attempting to communicate without authority were neither marked nor classified owing to an administrative oversight. In *Lim Kit Siang*,[38] the Malaysian High Court held that, "... classification of information is purely for administrative purpose and wrong classification on the part of the Government does not render information less secret."

In *Bridges Christopher*, the converse situation occurred. Bridges was convicted by the District Court of three charges of receiving information relating to change of addresses in contravention of the Act; and three charges of communicating the same information obtained in contravention of the Act to an unauthorised person. It was admitted that the information was given to Bridges by the co-accused, a field intelligence officer with the Criminal Investigation Department. The prosecution had led evidence to show that the information was obtained by the co-accused through the National Registration Office's on-line screening facilities. Such information obtained from the on-line screening facilities was classified as "secret" or "confidential".[39]

At the appeal, the learned Chief Justice held that the way the government chooses to treat the information is generally of little value in determining whether it is considered protected information under the Act:

> ... there is a boundary somewhere ... such that information falling on the wrong side of the line cannot be secret official information within the meaning of the Act no matter how the government chooses to treat it.[40]

[37] *Supra*, note 13. See also *Manu s/o Bhaskaran* v *PP* Magistrate's Appeal No 79/94/01, 29 August 1995 (Subordinate Courts, unreported), where the document in question, the Monetary Authority of Singapore Monthly Report, was not graded confidential as it was still in draft form.

[38] *Supra*, note 25, at 40 (HC).

[39] *Supra*, note 12, paras 11-13 (HC).

[40] *Ibid*, para 23 (HC).

The two situations are, however, not directly comparable. Where a piece of information or a document is not classified, it is no doubt correct that it is still open to the prosecution to show that the description of the information or document falls within paragraphs (a) to (e) of section 5(1) of the Act. Classification, or lack thereof, is after all an administrative act, unrelated to the criminal liability under the Act. However, where the information or document is classified, four reasons can be offered for giving greater deference to the Government's determination of the issue.[41]

First, unlike the former situation, the Government has spoken with regard to the sensitivity of the information or document. Deference, it may be argued, ought to be given to the opinion of the damaging effect of publication of the information or document. The approach of the courts in another bastion of official secrecy and reticence, that is, suppression of evidence relating to affairs of the State in litigation, may be usefully examined. In *Chan Hiang Leng Colin* v *PP*,[42] the appellants challenged the de-registration of the Jehovah's Witnesses as a society by the Minister for Home Affairs[43] and the prohibition of publications[44] which the appellants were found with as being contrary to the freedom of religion guaranteed by Article 15 of the Singapore Constitution. In doing so, the appellants also applied for an order directing the production of the files and documents of the respective ministries relating to the orders for de-registration and prohibition of publications.

The learned Chief Justice responded that:

> ...I quote with approval, the maxim *'salus populi est suprema lex', ie*, the safety of the people is the supreme law. Having heard the submissions of both counsel, I was not convinced ... that the public interest dictated that such documents be produced before this court. The importance of preserving the confidentiality of state papers need not be stressed.[45]

Secondly, the judiciary may be said to be too removed from the realities of administration or the needs for security to be allowed to second guess

[41] See the view of the Federal Court in *Lim Kit Siang* v *PP* [1980] 1 MLJ 293, 298 (FC), "[t]he Government has certainly the right to classify all this information as secret, the disclosure and utilisation of which would bring down the sanction of the law ..."; Franks Committee Report, *supra*, note 4, paras 145, 146.

[42] [1994] 3 SLR 662.

[43] Under s 24(1) Societies Act (Cap 311, 1985 Rev Ed).

[44] Under ss 3, 4(2) Undesirable Publications Act (Cap 338, 1985 Rev Ed).

[45] *Supra*, note 42, at 678. See ss 125, 164 Evidence Act (Cap 97, 1990 Ed); TY Chin, "Documents on 'Affairs of State' as Evidence" (1979) 21 Mal LR 24.

the nature of the information or document. Thirdly, information which may appear to be trivial or useless may very well be of strategic importance or the missing piece of the jigsaw sought by some hostile agency or group. Fourthly, that it is not sufficient for the court to sit *in camera* for such matters, since the secret evidence will be disclosed to the accused and his legal advisers present.

It was also the opinion of the Franks Committee that the determination of whether any information deserves protection should be left to the executive:

> ...the question of injury to the nation is essentially political, in the broadest sense of the term, not judicial. It is essentially a Government responsibility to assess the importance of information .... The Government is accountable to Parliament and the electorate for its discharge of these basic functions. Any system which placed this responsibility elsewhere would detract from the responsibility of the Government to protect the security of the nation and the safety of the people. It would remove the element of constitutional accountability.[46]

It is to the credit of the learned Chief Justice in *Bridges Christopher*[47] not to be swayed by these considerations and to hold that the ultimate determination whether the information is protected under the Act is one for the judiciary and not the executive. Giving the executive final say over such matters suffers from four serious shortcomings. First, it fails to consider the danger of abuse by the executive. The hollowness of the argument of "constitutional accountability" is shown by the *Ponting* case where the British Government was reluctant to disclose all information to Parliament which was embarrassing to itself and even allegedly misled members of Parliament.[48]

Secondly, the net of criminal liability may be cast unacceptably wide, extending to cases where no danger to the public is conceivable from the dissemination of such information. Thirdly, it may operate unfairly in that no fair notice is given to persons handling information which is not expressly

[46] Franks Committee Report, *supra*, note 4, para 145.

[47] *Supra*, note 12 (HC).

[48] See *infra*, note 145 and accompanying text. For Indian examples of the dangers of confidentiality in government, see VR Krishna Iyer, *Freedom of Information* (1990).

[49] The reasonable and legitimate expectations of an offender as to the state of the criminal law had been acknowledged by the Court of Appeal in *PP* v *Manogaran s/o R Ramu* [1997] 1 SLR 22, 42-43.

classified but the executive later claims it to be protected under the Act.[49] And finally, giving the executive final say over such matters fails to give any recognition at all to the role of the individual in the process of government.

It is unfortunate that the learned Chief Justice undercut his general proposition that "information falling on the wrong side of the line cannot be secret official information ... no matter how the government chooses to treat it" by recognising two situations where he is prepared to accept that information may be protected under the Act if it is so treated by the government:

(1) Where information is supplied to the government by private persons which the government has a duty to protect from indiscriminate disclosure;[50] and

(2) Where information is not formally released to the public but is of so innocuous a nature that nobody thought it necessary to do so formally.[51]

The first exception may be justified on a privacy rationale, but its formulation is too wide in that it may include information which the Government itself decides should be kept confidential. The second exception is difficult to comprehend. Where the information is innocuous, surely that must be "on the wrong side of the line". These exceptions only indicate the pressing need for a more coherent approach to determining what information should be considered protected under the Act.[52]

V. Implied Authorisation to Communicate

In *R* v *Galvin*,[53] the English Court of Appeal rejected the argument that section 2(1)(a) of the (UK) Official Secrets Act 1911 (*ie,* having in his possession any document which was obtained owing to his position as a person who holds a contract made on behalf of Her Majesty, communicates the document to any person, other than a person whom he is authorised

[50] *Supra*, note 12, para 27 (HC).

[51] *Ibid*, para 33 (HC).

[52] See also *ibid*, para 40 (HC), where the learned Chief Justice says, "...if a department treats that information as 'confidential' or 'secret' or in any other way which makes it clear that it should not be released or made available to the public, the information is secret official information under the Act. *It is, after all, not the function of the courts to second-guess the government.*" (emphasis added)

[53] *Supra*, note 10.

to communicate it) did not apply if the information is already made public and had come within the public domain. Instead, it was decided on the basis that if the information had been made public by the Government itself, the communication may have been impliedly authorised, and therefore, not an offence.

The operation of the phrase "person to whom he is authorised to communicate" in section 2(1)(a) of the (UK) Official Secrets Act 1911 had been understood to include express as well as implied authorisation. Hence, the communication of official information is proper if such communication can be fairly regarded as part of the job of the officer concerned. Ministers and senior civil servants may decide what disclosures of official information they may properly make.[54]

This approach was apparently rejected in *Bridges Christopher* by the learned Chief Justice where he said that, "there can hardly be an implied authority to disclose something expressly classified as 'Top Secret'".[55] The judgment, however, was not internally consistent. The concept of implied authorisation was still referred to in a later passage:

> ... if a department treats that information as 'confidential' or 'secret' or in any way which makes it clear that it should not be released or made available to the public, the information is secret official information under the Act. ...if, however, some other department, which is authorised to release this information or make it available to the public, does not expressly treat it as confidential or secret, and someone from that department releases the information or makes it available to the public, the release of this information could be treated as impliedly authorised.[56]

The proper role of implied authorisation within the structure of the Act still needs to be resolved. In *Phua Keng Tong*,[57] one of the accused (Tan) was a senior official in the Ministry of Foreign Affairs charged with three counts of communicating or attempting to communicate documents to Phua, an unauthorised person contrary to section 5(1)(e)(i) of the Act. In his defence, Tan said that in his official capacity at the Ministry, it was a common practice when posted abroad to do "trading" of documents which do not affect the

54 Franks Committee Report, *supra*, note 4, paras 18, 33, 35.
55 *Supra*, note 12, para 23 (HC).
56 *Ibid*, para 40 (HC).
57 *Supra*, note 13.
58 *Ibid*, at 285.

security of the State, and that in his present position, he would evaluate documents or information which he could provide to the press.[58]

Those situations were not relevant in the instant case and were not considered by the Court. However, in an appropriate case, the Court may be pressed to decide if the practice referred to or the giving of information to the press may or may not amount to an offence under the Act owing to "implied authority" to communicate that information or document arising from the accused's position and function. It is submitted that the role of implied authorisation should be recognised in appropriate cases.

VI. "INFORMATION" VS "DOCUMENT"

Section 5 of the Act protects the information itself (code word, countersign, password or information) as well as the item containing the information (photograph, drawing, plan, model, article, note, document). In *Datuk Haji Dzulkifli Bin Datuk Abdul Hamid* v *PP*,[59] the accused was charged with, *inter alia*, receiving or communicating secret official information or, alternatively, secret official document contrary to the Malaysian Official Secrets Act. Although the information was publicly known, the accused was nevertheless convicted of the alternative charges. An argument that the information and the document containing it are inseparable was rejected. This was explained by the learned Chief Justice in *Bridges Christopher*:

> [T]he fact that the information contained in the documents is in the public domain is considered to be irrelevant. This is because, regardless of what information is contained in the document, the document itself had not been released or made available by any arm of the government to the public.[60]

Similarly, in *Phua Keng Tong*,[61] the fact that "substantially, the contents of the documents were already known to those informed of current events and could hardly be of any assistance to anyone engaged in trading in currencies" was only a factor to be taken into consideration in sentencing and not in ascertaining liability under the Act.

It is submitted that this approach creates an unreal distinction between the "information" and the item containing it. If the information itself is not considered protected because it is widely known or released by the

[59] [1981] 1 MLJ 112.
[60] *Supra*, note 12, para 32 (HC).
[61] *Supra*, note 13, at 285.

relevant authority, it should not be an offence under section 5 of the Act to communicate a document containing the same information. If the mischief aimed at in the latter case is the unlawful manner in which the document is obtained, the proper avenue of redress is through the disciplinary process for civil servants. If a criminal charge is nevertheless felt justified, the better charge is that of theft or criminal breach of trust under the Penal Code.[62]

Reference to the specific legislation dealing with unauthorised communication of particular information provided by the public under statutory requirements also reveal that it is the communication of the information itself, and not the item containing it, that is regulated.[63]

The reason for this distinction made between "information" and "document" is the fear that:

> ...it makes no sense of the secrecy of examination papers and even ... draft judgments before they are released, as the information contained therein can openly be found elsewhere, in textbooks, periodicals, magazines and newspapers. In our view such a contention is totally unacceptable.[64]

The learned Chief Justice in *Bridges Christopher*[65] explained that examinations and draft judgments remain protected because it is the *fact* that certain information is contained therein is secret and not because the information itself is secret. However, the public interest justifying the use of criminal, rather than administrative, sanctions for breach of secrecy in such cases

[62] Ss 378, 405 Penal Code (Cap 224, 1985 Rev Ed). The document would certainly be "movable property" for the purposes of theft: s 22 Penal Code (Cap 224, 1985 Rev Ed).

[63] *Eg*, ss 19(e), 20(f) Census Act (Cap 35, 1991 Rev Ed); s 59(1) Central Provident Fund Act (Cap 36, 1994 Rev Ed); s 25(2), (3) Control of Imports and Exports Act (Cap 56, 1985 Rev Ed); s 90D(2), (3) Customs Act (Cap 70, 1995 Rev Ed); s 102(2), (4) Employment Act (Cap 91, 1996 Rev Ed); s 6(2) Goods and Services Act (Cap 117A, 1997 Rev Ed); s 6(2) Income Tax Act (Cap 134, 1996 Rev Ed); s 11 Nursing Homes and Maternity Homes Registration Act (Cap 210, 1985 Rev Ed); s 4 Public Service Commission Act (Cap 259, 1985 Rev Ed); s 9(5) Sale of Drugs Act (Cap 282, 1985 Rev Ed).

[64] *Datuk Haji Dzulkifli, supra*, note 59, at 113.

[65] *Supra*, note 12, paras 21, 22 (HC). A homely example was given at para 21: "Thus, the contents of an examination paper may be secret official information until the examination. '1 + 1 = 2' is not secret official information, but the fact that that question is asked, and the answer expected, in the paper is."

is difficult to comprehend.

VII. *Mens Rea* under Section 5(1) of the Act

Section 1(1)(b) of the first (UK) Official Secrets Act 1889 originally provided that:

> Where a person **knowingly** having possession of, or control over, any such document, sketch, plan, model, or knowledge as has been obtained or taken by means of any act which constitutes an offence against this Act at any time **wilfully** and without lawful authority communicates or attempts to communicate the same to any person to whom the same ought not, in the interests of the State, to be communicated at that time ... shall be guilty of a misdemeanor .... (emphasis added)

The *mens rea* words in bold above were not included in the later section 2(1)(a) of the (UK) Official Secrets Act 1911 or in section 5(1)(c)(i) of our Act.[66] By leaving out these words, it may be argued that the legislature intended to create a strict liability offence. Comparison can also be made with section 2(2) of the (UK) Official Secrets Act 1911 and section 5(2) of our Act where it is expressly stated that the accused must know, or have reasonable ground to believe, at the time of receiving the information, that it was being communicated in contravention of the Official Secrets Act.

There have been at least two previous decisions in the UK describing the offence as an "absolute" one not involving any element of guilty knowledge.[67] It has also been accepted in Malaysia *obiter* that the offence under section 8(1) of the Malaysian Official Secrets Act, which is *in pari materia* with section 5(1) of our Act, is an absolute one.[68] This uncertainty has since been clarified in the local cases. In *Phua Keng Tong*,[69] it was held that for the purpose of an offence under section 5(1)(e)(i) of the Act, "the *mens rea* is a knowledge of the wrongfulness in committing the act complained of". In *Bridges Christopher*, it was elaborated that in relation to section

66 *Cf* s 5(1)(a) The Indian Official Secrets Act (Act XIX of 1923) which requires the person to "wilfully" communicate *inter alia* the information to any person other than a person to whom he is authorised to communicate it.

67 Franks Committee Report, *supra*, note 4, para 20. See also *R* v *Fell* [1963] Crim LR 207; and the trial of Auberry, Berry and Campbell noted in Andrew Nicol, "Official Secrets and Jury Vetting", *supra*, note 10; Rosamund Thomas, "The British Official Secrets Acts 1911-1939 and the Ponting Case" [1986] Crim LR 491, 500-501. The uncertainty about the requirement of *mens rea* for this offence was criticised in Franks Committee Report, *supra*, note 4, para 218.

68 *Lim Kit Siang, supra*, note 25, at 42 (HC).

69 *Supra*, note 13, at 284.

5(1)(c)(i) of the Act, the mental elements required are:

(1) an intention to communicate the information;

(2) knowledge that the information was obtained by the communicator in contravention of the Act; and

(3) knowledge of the communicator that he had no authority to communicate the information to the person to whom he communicated it or that he had no duty to communicate it to the person he communicated it.[70]

The above position was arrived at by reference to the general rule that *mens rea* is presumed to be a necessary ingredient of an offence in the absence of clear words to the contrary.[71] It was also noted that the mere possession of protected information does not constitute an offence under section 5(1) of the Act, but only if the person further communicated, used, retained or failed to take reasonable care of the information as provided in paragraphs (i) to (iv). Each of these other acts require a mental element.[72] The prosecution's argument that the object of promoting the protection of State secrets by construing the provision as a strict liability offence was rejected as being unpersuasive by the learned Chief Justice in the High Court.[73]

It should be noted that the burden of proof of unauthorised communication in limb (3) above is put squarely on the prosecution. It was not regarded as a defence under section 107 of the Evidence Act.[74] However, there is no need to show a further intention to prejudice the State in any way.[75]

[70] *Supra*, note 8, para 46 (CA). There is no requirement for knowledge that the information is secret official information, *cf* the High Court decision, *supra*, note 12, para 74 (HC), since the Court of Appeal had decided that the phrase "secret official" did not qualify "information".

[71] See criticisms of this approach in the local context in Michael Hor Yew Meng, "Strict Liability in Criminal Law: A Re-Examination" [1996] SJLS 312, 332-338.

[72] *Supra*, note 8, para 45 (CA); *Phua Keng Tong*, *supra*, note 13.

[73] *Supra*, note 12, paras 70, 71 (HC).

[74] Cap 97, 1990 Rev Ed.

[75] This is unlike the offence of spying under s 3(1) Official Secrets Act (Cap 213, 1985 Rev Ed) where acting for a "purpose prejudicial to the safety or interests of Singapore" is needed.

[76] *Supra*, note 12, para 72 (HC), approving *Chandler* v *DPP* [1964] AC 763, 793; *Phua Keng Tong, supra*, note 13, at 284.

This is a motive, which is irrelevant to the requisite *mens rea* of the offence under paragraph (i) to section 5(1).[76]

It is however unclear in the above formulation if only actual knowledge suffices for limbs (2) and (3) or whether it will be sufficient if the communicator knows or has reasonable grounds to believe thus. The learned Chief Justice in the High Court formulated limb (2) as "know or have reasonable grounds to believe that the information or thing was communicated in contravention of the Act".[77] The Court of Appeal too, in the very next passage, said:

> The prosecution's evidence at the close of its case, in so far as Bridges was concerned, fell short of establishing a *prima facie* case that Bridges had knowledge of the source from which Ganesan had obtained the information. *In other words, there was no evidence on which it could reasonably be inferred that Bridges knew or had ground to believe that he, Bridges, was in possession of 'protected' information which was obtained by Ganesan and communicated to him in contravention of the Act.*[78] (emphasis added)

The common law presumption of *mens rea* doctrine typically involves two choices: either *mens rea* is a constituent element of the offence; or a legislative intention to displace the *mens rea* requirement can be inferred. With respect of the former, it is the full *mens rea* that is imputed, namely, knowledge of a state of affairs.[79] Liability on the basis whether a reasonable man in the offender's shoes would have known a state of affairs had not been imputed through this doctrine. The High Court and the Court of Appeal have extended the limits of this doctrine by suggesting that actual knowledge or "reasonable ground to believe" are alternative *mens rea* for limb (2) above.

However, it is submitted that construing the *mens rea* requirement as "knowing or having reasonable ground to believe" in both limbs (2) and (3) brings a greater coherence to the offences under section 5(1) and (2) of the Act. Under section 5(2) of the Act, it is specifically provided that an offence is committed if the person receives *inter alia* information knowing or having reasonable grounds to believe that it was communicated in contravention of the Act. Actual knowledge is not required.[80] Hence, the same *mens rea* should apply for an offence under section 5(1) of the Act.

[77] *Supra*, note 12 para 78 (HC).
[78] *Supra*, note 8, para 47 (CA).
[79] *Eg, Gammon (Hong Kong) Ltd* v *AG of Hong Kong* [1985] AC 1.
[80] *Supra*, note 12, paras 49, 50 (HC), distinguishing *Phua Keng Tong, supra*, note 13.

The requirement of "knowing or having reasonable grounds to believe" balances the concerns that criminal liability may be extended too far with the need for an efficient system for the protection of information. A person will have "reasonable grounds to believe" if he has "sufficient cause to believe that thing" based on the evidence adduced at the trial.[81] This level of guilt has been described as a mental state which "involves a lesser degree of conviction than certainty and a higher one than speculation".[82] Whether a person has "reason to believe" a fact is a test applied by the Court but from the perspective of the accused person, taking into account any specialised knowledge or experience he may have. Hence, it is highly relevant to the assessment by the Court if the accused, for example, had been a former civil servant.[83]

VIII. Circumstances Relevant to Inferring Knowledge

A range of circumstances had been recognised by the courts in finding that a party either knew or had reasonable grounds to believe that the information was obtained in contravention of the Act. These include:

(i) Nature of the information, namely, if it is obviously of a confidential character.[84]

In *Lim Kit Siang*,[85] the information revealing the exact number of tenderers for supply of naval craft to the Royal Malaysian Navy; the identity of the short-listed tenderers and the successful tenderer; the original and final prices submitted; the mode of payment and cost of the crafts were held by the Malaysian High Court as indicating that the information could not have come from one of the tenderers or

81 S 26 Penal Code (Cap 224, 1985 Rev Ed); *Bridges Christopher, supra*, note 8, para 41 (CA).

82 *Koh Hak Boon* v *PP* [1993] 3 SLR 427, 430.

83 *Infra*, at Part VIII.

84 *Bridges Christopher*, *supra*, note12, para 57 (HC); see also *R* v *Crisp and Homewood, supra*, note 10; and *Datuk Haji Dzulkifli, supra*, note 59, at 113: "It is common sense that such [information] should be kept secret."

85 *Supra*, note 25, at 41-42 (HC).

a person other than someone from the Government.

(ii) Circumstances in which the information is received.

In *Lim Kit Siang*,[86] one of the circumstances referred to was that the communication by way of an anonymous letter ought to have aroused suspicions that the writer was communicating information unlawfully obtained.

(iii) Time in which information is communicated.

Information relating to contracts for the supply of officers' uniforms in *Crisp and Homewood*[87] was supplied at a time when the United Kingdom was in the midst of the First World War.[88]

(iv) Where an undertaking was given or declaration made to safeguard official information.[89]

(v) Occupation and position of the accused.

In *Phua Keng Tong*,[90] the fact that one of the accused (Tan) had been in the Government service since 1966 and at the material time held a senior position in the Ministry of Foreign Affairs was found relevant.

The *previous* position of the accused in the Government service may also be referred to in inferring the requisite knowledge. In *Manu s/o Bhaskaran* v *PP*,[91] it was noted that the second accused had served in the Security and Intelligence Division of the Ministry of Defence for some nine years before joining the private sector; and in *Datuk Haji Dzulkifli*,[92] the accused was a former civil servant and a former

86 *Ibid*, at 43.
87 *Supra*, note 10.
88 As explained in *Bridges Christopher, supra*, note 12, para 56 (HC).
89 *PP* v *Bridges Christopher* Magistrate's Appeal Nos 159/96/01-02, 19 August 1996 (Subordinate Court, unreported); *PP* v *Ronnie Wong Peng Kong* Magistrate's Appeal No 158/96/01, 11 June 1996 (Subordinate Court, unreported); *Phua Keng Tong, supra*, note 13.
90 *Ibid*, at 284.
91 *Supra*, note 37. See also *Phua Keng Tong, supra*, note 13, where the accused Phua had been in the Government service for about 3 years and held a senior position at the time he left the service.
92 *Supra*, note 59.

Minister in the Government.

(vi) Manner in which the accused handled the information.

In *PP* v *Ronnie Wong Peng Kong*,[93] the information was recorded in his police pocket book in a detailed manner and he had consulted his superior about it.

(vii) Security markings on the document

In *Datuk Haji Dzulkifli*,[94] the letter "S", which stands for the word "secret", typed in front of the reference number was held sufficient to show that the document was protected. This is so even though the document was not classified as "Rahsia" (secret). In *Phua Keng Tong*,[95] it was pointed out that even if the document was overclassified, this only showed that the document was meant for circulation or distribution to persons authorised to receive it.

However, some circumstances found to be insufficient to give rise to a reasonable cause to believe that the information is communicated in contravention of the Act include:

(i) Source of the information where the information is generally available from some other government department.

In this situation, the mere fact that the information is divulged by a person working in the government is not sufficient to show that there is ground for believing that the information was revealed in contravention of the Act.[96]

(ii) Difficulty in obtaining the information from other sources.

Where the information can only be obtained through a tedious process or through payment of money, the fact that a person is able to supply the same information quickly and without charge is not a sufficient basis to infer a reasonable ground of belief that the information is

[93] *Supra*, note 89.
[94] *Supra*, note 59.
[95] *Supra*, note 13, at 286.
[96] *Bridges Christopher, supra*, note 12, paras 58, 61, 62 (HC).
[97] *Ibid*, paras 64-66 (HC).

obtained unlawfully.[97]

IX. Receiving Information under Section 5(2) of the Act

There is no requirement under section 5(2) of the Act that the protected information be intentionally received. It had been held that receipt of information refers purely to the act of acquiring knowledge of the information. Hence, information may be received merely by sighting it, whether it was advertent or not.

In *Manu s/o Bhaskaran*,[98] the second accused was found to have sighted the Flash Estimate of 4.6% growth for the Singapore economy in the second quarter of 1992 from a document placed opposite him at a meeting with the first accused, the Director of the Economics Department of the Monetary Authority of Singapore. This was held sufficient for the offence under section 5(2) of the Act even though he had not intentionally sought to acquire that piece of information.

However, a defence to criminal liability under section 5(2) of the Act exists if the defendant can show that the information was communicated contrary to his desire. This is a limited defence in that the fact that the accused did not specifically request for a certain document or that the particular information is of no use to the accused in actual fact does not automatically mean that the communication was contrary to his desire. In determining this factor, the court may consider the accused's prior conduct and agreement with any other party[99] as well as his subsequent actions upon receipt of the information.[100]

Hence, in *Phua Keng Tong*,[101] the prior agreement between the two accused, Phua and Tan, to try to recoup their losses in foreign currency speculations by engaging in further trades showed that even though the particular document concerning political developments in Japan was not asked for by Phua, and that the information was in fact stale and of no use, did not amount to it being contrary to Phua's desire to receive it for the purposes of section 5(2) of the Act. Similarly, in *Lim Kit Siang*,[102] the fact that the information was given by way of an anonymous letter and not sought by the accused was not relevant considering the extent to which

[98] *Manu s/o Bhaskaran, supra*, note 37, at 46, 55.
[99] *Phua Keng Tong, supra*, note 13, at 287.
[100] *Manu s/o Bhaskaran, supra*, note 37, at 66.
[101] *Supra*, note 12, at 287.
[102] *Supra*, note 41, at 298 (FC).

the accused had made use of the information by communicating it to various unauthorised persons.

Thus, a distinction has been made in the case law between receiving information contrary to his intention and contrary to his desire.[103] Catching sight of a document inadvertently may be contrary to his intention but may not be contrary to his desire. It is submitted that the offence under section 5(2) of the Act would have been clearer if the former phrase in the Official Secrets Ordinance 1935 were retained, "unless he proves that the reception by him of the said information or thing was not directly or indirectly solicited by him".[104]

X. Communication under Section 5(1) and (2) of the Act Compared

The learned Chief Justice in *Bridges Christopher*[105] interpreted the word "communication" in section 5(1) of the Act to connote intention. Hence, an intention to communicate the information must be shown. If the same meaning is applied to the word "communicate" in section 5(2), and there is no reason why it should not,[106] a case such as *Manu s/o Bhaskaran*[107] may have to be decided differently today.

In that case, the second accused was charged with *inter alia* receiving information, namely the Flash estimate of Singapore's second quarter economic growth in 1992, at a meeting with the first accused and others. However, it was accepted that the first accused did not intentionally communicate the information to Manu. The first accused was instead convicted under

[103] *Manu s/o Bhaskaran, supra*, note 37, at 66.

[104] Paragraph (v) to s 4 Official Secrets Ordinance (No 25 of 1935).

[105] *Bridges Christopher, supra*, note 12, para 73 (HC). The Court of Appeal agreed, see footnote 70 and accompanying text. The Act itself fails to give any guidance on the need for *mens rea*. S 2(2) Official Secrets Act (Cap 213, 1985 Rev Ed) states: Expressions referring to –

> (a) communicating or receiving include any communicating or receiving, whether in whole or in part, and whether the photograph, drawing, plan, model, article, note, document or information itself or the substance, effect or description thereof is communicated or received. ...
>
> (c) the communication of any photograph, drawing, plan, model, article, note or document include the transfer or transmission of the photograph, drawing, plan, model, article, note or document.

[106] It is a principle of statutory construction that the same word in an Act should be given the same meaning throughout, unless a contrary intention appears, see FAR Bennion, *Statutory Interpretation* (2nd Ed, 1992) pp 806, 808.

[107] *Supra*, note 37.

[108] *Supra*, note 37, at 11.

section 5(1)(d)(iv) of the Act for so conducting himself as to endanger the secrecy of the information.[108] Hence the words "communicated to him" in section 5(2) of the Act was held not to require the communicator to do so intentionally.

It is submitted that the reason given by the District Court, that "communication" in section 5(2) only refers to the *actus reus* of communication whereas in section 5(1), the word refers to both the *actus reus* and *mens rea* of communication,[109] is not convincing. There is no reason in principle why the same word in the same section of the Act should be given such different meanings. If it is intended that an offence under section 5(2) of the Act should be committed in a case such as *Manu s/o Bhaskaran*,[110] it may be better to use the phrase "received by him" and "receipt" instead of "communicated to him" and "communication to him".

XI. Defence of Duty to Communicate Information

Under paragraph (i) to section 5(1) of the Act, there is a defence to the charge of unauthorised communication of protected information if "it is his duty to communicate it". The occurrence of the phrase "person to whom he is authorised to communicate it" immediately before, suggests that a wide reading is to be given to the concept of "duty". It must mean more than implied or express authority to communicate the information granted by the powers or duties of the person involved. It arguably allows the accused to invoke some higher duty to justify his conduct in overriding the Government's interests in protecting the information.[111]

In comparison, the equivalent UK provision, section 2(1)(a) of the (UK) Official Secrets Act 1911, reads, "... a person to whom it is **in the interests of the State** his duty to communicate it". The words in bold are not found in our Act. It is submitted that the duty in our provision should be similarly restricted, otherwise it may be too vague and uncertain if entirely personal interests can be appealed to. On the other hand, there is no need for such

[109] *Supra*, note 37, at 43-45.

[110] *Supra*, note 37.

[111] The English case law indicate little scope for the operation of the equivalent defence, see Yvonne Cripps, "Disclosure in the Public Interest: The Predicament of the Public Sector Employee" [1983] PL 600.

[112] *Cf Ponting* [1985] Crim LR 318, which adopted the views of Lord Devlin and Lord Pearce in *Chandler* v *DPP, supra*, note 76. For comment see Gavin Drewry, "The Ponting Case – Leaking in the Public Interest" [1985] PL 203; Rosamund Thomas, "The British Official Secrets Act 1911-1939 and the Ponting Case", *supra*, note 67, at 496-500.

interests to be confined to the interests of the Government of the day.[112] The defence should encompass disclosures made in the national interest lest information unfavourable to the Government, but of importance to the nation, be stifled.

In relation to the Malaysian provision, which also does not have the words in bold above, there has also been an effort to cut down the width of the duty. It was said that the duty must be a "duty as a Government servant that he owes to his superior or ministers"[113] or arise from one's duty as a citizen.[114] The circumstances in which such a duty can arise are necessarily limited:

> If therefore, a person should have in his possession any information which relates to some exigencies of particular importance to the country as a whole such as matters affecting the national calamity or catastrophe, it is undeniably his duty as a citizen to disclose to someone with the object that the calamity or catastrophe be avoided.[115]

At the same time, it is submitted that there is no need for the information concerned to be of such great magnitude before the use of the defence can be justified. It is suggested that the defence should operate by considering the purpose of the accused in disseminating the information. To do this, a *balancing process* should be used in comparing the nature of the information with the scope of dissemination of the information.

To this end, a comparison with the civil law of breach of confidence can be made. Cases from other jurisdictions such as *AG* v *Jonathan Cape Ltd*,[116] *AG* v *Guardian Newspapers (No 2)*[117] and *Commonwealth of Australia* v *John Fairfax & Sons Ltd*[118] show that the duty of confidentiality in the civil law may be used to restrain disclosure of Government secrets as well. In such situations of overlap between civil and criminal liability, it is desirable that the principles applied are as broadly similar as the circumstances allow.

[113] *Lim Kit Siang, supra*, note 25, at 42 (HC).
[114] *Ibid*, at 46.
[115] *Ibid*.
[116] [1976] QB 752.
[117] *Supra*, note 36.
[118] 147 CLR 39.
[119] *Gartside* v *Outram* (1856) 26 Ch 113. The public interest defence has been recognised in Singapore, *eg, X Pte Ltd* v *CDE* [1992] 2 SLR 996, 1009-1010.

A public interest defence has long been recognised against actions for breach of confidence.[119] In its present form, the touchstone of the defence is a balancing exercise of competing interests.[120] However, in the area of government secrets it is not just a matter of balancing the public interest in maintaining confidentiality against the public interest in exposing a breach of the law or "anti-social" activities.[121] There is also the matter of the legitimate interests of the citizens in the operations of the government. In the famous "Spycatcher" case, it was explained by Lord Goff:

> ...although in a case of private citizens there is a public interest that confidential information should as such be protected, in the case of Government secrets the mere fact of confidentiality does not alone support such a conclusion, because in a free society there is a continuing public interest that the workings of the Government should be open to scrutiny and criticism. From this it follows that, in such cases, there must be demonstrated that some other public interest which requires that publication should be restrained.[122]

Two rules developed in the law of confidence may be instructive. First, limitations are placed on the extent and degree of disclosure of information. Disclosures may only be justified to persons who have a proper interest to receive the information.[123] This is particularly relevant where there are proper avenues of complaint. In *Francome* v *Mirror Group Newspapers Ltd*[124] for example, the defendants obtained taped telephone conversations between the plaintiff, a well-known jockey, and his wife. The tapes revealed breaches of Jockey Club regulations and possibly criminal offences committed by him. The defendants intended to publish the material in the tapes. In relation to the action for breach of confidence, the English Court of Appeal ruled that the publication cannot be justified in the public interest since any public interest could be served by making the tapes available to the police or the Jockey Club.

Secondly, it has also been said that the mere allegation of iniquity is not of itself sufficient to justify disclosure in the public interest. Such an

[120] But see criticisms of this approach in *Smith Kline and French Laboratories (Australia) Ltd* v *Secretary, Department of Community Services and Health* (1990) 17 IPR 545, 583; *Corrs Pavey Whiting and Byrne* v *Collector of Customs for the State of Victoria* (1988) 10 IPR 53.

[121] *Francome* v *Mirror Group Newspapers Ltd* [1984] 2 All ER 408.

[122] *Supra*, note 36, at 283.

[123] *Initial Services Ltd* v *Puterill* [1968] 1 QB 396; *X Pte Ltd* v *CDE, supra*, note 119, at 1009.

[124] *Supra*, note 121.

allegation will only do so if, following such investigations as are reasonably open to the recipient, and having regard to all the circumstances of the case, the allegation in question can reasonably be regarded as being a credible allegation from an apparently reliable source.[125]

Considering the repercussions of a criminal conviction, the scope of the public interest defence in the Act can be no less. It should be sufficient if the defence shows that the accused had *reasonable cause to believe* that the information indicated the existence of crime, fraud, abuse of authority, neglect in the performance of an official duty or other misconduct and that the scope of disclosure of the information was *reasonable* to draw such misconduct to the attention of the appropriate authorities.

This does not amount to a blanket protection for any unauthorised disclosure of information based on a tenuous suspicion of impropriety on the part of the Government. There must, in addition, be an objective assessment of the credibility of the information and justification for the extent of its publication. Hence, the Malaysian High Court in *Lim Kit Siang*[126] was right to cast doubt on the veracity of accusations of impropriety made in an anonymous letter by an unknown person. Some reason for accepting the accuracy of the accusations of impropriety must be shown. The local and Malaysian cases indicate that there is scope for such development.

In *Ronnie Wong Peng Kong*,[127] the information received over the telephone suggested that the accused's subordinate was being wrongly investigated by the Corrupt Practices Investigation Bureau ("CPIB") for a corruption offence. The information was recorded in a police pocket book and a photocopy of it was given to the subordinate.

In *Datuk Haji Dzulkifli*,[128] a former Minister wanted to contradict what was reported to have been said by the Chief Minister of Sabah on the State's policy on Philippine refugees by leaking a copy of a letter written by the former Chief Minister to the Minister of External Affairs. The letter was given to a journalist and a chief editor of the Kinabalu Sabah Times and it was subsequently published.

In *Lim Kit Siang*,[129] the Member of Parliament and Leader of the Opposition possessed information on the award of a tender for the purchase of four

[125] *AG* v *Guardian Newspapers (No 2), supra*, note 36, at 283. The limitation, however, will not apply if the disclosure is to a recipient who has a duty to investigate the matters raised, *In re A Company's Application* [1989] IRLR 477.
[126] *Supra*, note 25, at 46 (HC).
[127] *Supra*, note 89.
[128] *Supra*, note 59.
[129] *Supra*, note 25.

naval craft for the Royal Malaysian Navy suggesting serious misconduct on the part of the Tenders Board of the Ministry of Defence.

It is submitted that in each of these cases, the defence could have been made out if the information had been revealed to the proper authorities, and via proper channels. In *Ronnie Wong Peng Kong*,[130] it was recognised that there is a public interest in the administration of justice requiring the information to be ultimately available to the court hearing the corruption charge. The only complaint is that the information ought to have been conveyed to the CPIB, instead of to the subordinate. In *Lim Kit Siang*,[131] the Federal Court pointed out that no prosecution would have followed if he had not disseminated the information further than by writing to the Prime Minister.

XII. Burden and Standard of Proof

It is axiomatic that the prosecution bears the burden of proof in the prosecution of any offence. In relation to section 5(1) of the Act, the prosecution must show that the information comes within one of the paragraphs (a) to (e) and has been used in one of the ways specified in paragraphs (i) to (iv) of the subsection.[132] From the Court of Appeal's answer to the third question of law referred to it, it is also clear that the prosecution must, in addition, show that the information has not been published, released or made available to the public by a person authorised to do so.[133]

However, an unrealistically high standard of proof appears to have been adopted in the application of the above. The learned Chief Justice in *Bridges Christopher* seems to have required that the prosecution not merely show that the information was not publicly available, but that there was no possibility that the information was so available. In that case, the prosecution was faulted for not eliminating the possibility that the current addresses

[130] *Supra*, note 89.

[131] *Supra*, note 41, at 297 (FC).

[132] *Bridges Christopher, supra*, note 8, paras 35-39 (CA). This is relevant to both s 5(1) and (2) since the offence under s 5(2) is committed if *inter alia* the information is received knowing or having ground to believe that the information is communicated to him *in contravention of the Act.*

[133] *Ibid*, paras 39, 60 (CA). The third question was: "In a prosecution for an offence under s 5 of the OSA, notwithstanding that the burden lay on the prosecution to prove that the information falls within s 5, whether the prosecution has to prove that the information has not been published, released or made available to the public by a person authorised to do so".

[134] Ss 10(3), 15(2) Parliamentary Elections Act (Cap 218, 1995 Rev Ed).

were obtained from the electoral registers, which are available to the public by law.[134] The difficulty of tracing the addresses of persons through this means, since the entries are arranged by constituency and street names rather than by name or identity card numbers, was rejected:

> There is nothing to prevent someone from buying the complete collection of registers and scanning the information into a computer database. And even if there is, there is nothing to prevent someone stumbling on the addresses from publishing it in whatever manner he pleases.[135]

> Sheer volume of information released with authority does not turn any part of the released information into secret official information.[136]

As to the argument that the electoral registers do not provide the dates of the change of addresses, the learned Chief Justice responded that the dates of the changes can be estimated by comparing the different editions of the registers and it would be "indulging in speculation" that the information cannot be obtained from the Registration Officer.[137] The Court of Appeal did not comment on the application of the standard of proof by the High Court as it was only concerned with the questions of law referred to it.

The approach of the learned Chief Justice may be contrasted with *Lim Kit Siang* in Malaysia where the accused was charged with, *inter alia*, receiving and communicating secret official information relating to the Federal Government's purchase of four naval craft. The Federal Court dismissed the appellant's argument that the information could have come from non-governmental sources such as the tenderers for the contract and those connected with the successful tenderer:

> ... we are not greatly enamoured with this argument.... Apart from considerations of the burden on the prosecution in any criminal case to establish a case against the accused not beyond absolute doubt but only beyond reasonable doubt and the onus of proof to establish the source of the information, there is no truth in the suggestion that the appellant derived his information from non-government or non-secret sources. The immense difficulty, nay, the impracticability in tracing all the tenderers and ascertaining from them whether they were successful

[135] *Supra*, note 12, para 38 (HC).
[136] *Supra*, note 12, para 65 (HC).
[137] *Supra*, note 12, para 44 (HC).

> or not, and finding out by a process of elimination the short-listed tenderers, and the absence of any credible reason for the successful tenderer to venture information of the details of its tender must clearly seen to be the short answer to the suggestion.[138]

It is submitted that in order to achieve a fair balance between the competing interests of the prosecution and the accused person, it should be sufficient for the prosecution to show that the information could not *reasonably* be compiled from publicly available sources. That ought to raise a *prima facie* case that the information was not obtained from an authorised source sufficient for the defence to be called.[139]

In any case, at the material time in *Bridges Christopher*, the latest electoral registers available were those for 1992. However, the information involved changes of addresses made in respect of three of the four persons in 1993![140] This alone would have shown that the information could not have been derived from the 1992 electoral registers.[141]

XIII. Emerging Principle: Harm Analysis

The care with which the High Court and the Court of Appeal in *Bridges Christopher* have limited the scope of information which can be protected under the Act indicate that there is a need for a clear principle for circumscribing the apparently wide liability under section 5 of the Act.

It is suggested that a principle underlying the judgments in *Bridges Christopher* is a need to show that the information involved is of a nature

[138] *Supra*, note 41, at 297 (FC).

[139] *Cf Bridges Christopher, supra*, note 12, paras 42, 44 (HC).

[140] *Ibid*, paras 8, 9 (HC).

[141] The new addresses would of course be reflected in the 1996 electoral registers but this, it is submitted, is irrelevant to the issue whether the information is satisfactorily shown to be protected under the Act at the time of the commission of the offence, *ie*, in 1993. *Cf Bridges Christopher, supra*, note 12, para 39 (HC). The sensitivity of a piece of information may change with time but it would be unthinkable that an offence cannot be committed with respect to an unauthorised disclosure of say military intelligence if it were to be subsequently declassified and released to the public in peacetime.

[142] The requirement for harm to be shown from the disclosure of protected information is also in line with the present UK legislation, the Official Secrets Act 1989. Different levels of harm are required for different categories of information.

[143] *Supra*, note 89, at 110. The learned Chief Justice in *Bridges* accepted, but without expressly ruling on the issue, that addresses could be protected information, *supra*, note 12, para 34 (HC).

that may result in serious damage or risk of serious damage to the interests of the State.[142] Hence, the Subordinate Court in *Bridges Christopher*[143] noted for the purposes of sentencing that the information concerned, namely addresses and the dates of change of addresses of individuals, was not sensitive. The fact that such information is available from other sources, for example, the National Registration Office (until November 1985), Land Transport Authority, Registry of Companies and Businesses, the electoral registers and commercial sources such as Creditnet Pte Ltd supports this conclusion. Furthermore, the information had been ultimately used for the purpose of serving legal documents on defendants who had been trying to dodge the justice system.

The development of a harm criterion locally stands in sharp contrast with the approach under the former (UK) Official Secrets Act 1911. A previous British Attorney-General had commented that section 2 of their (UK) Official Secrets Act 1911:

> [M]akes it a crime, without possibility of a defence, to report the number of cups of tea consumed per week in a government department, or the details of a new carpet in the minister's room.... The Act contains no limitation as to materiality, substance, or public interest.[144]

Three responses may be made. First, the interpretation given to section 2 of the (UK) Official Secrets Act 1911 was given extra-judicially, and it need not restrain the local courts from forging our own understanding of the scope of criminal liability under our Act.

Secondly, there is a danger in divergence between wide liability imposed by the Act and the public perception of wrongdoing. In the *Ponting* case in England,[145] the accused was, at the material time, assistant secretary in the Ministry of Defence dealing with naval operations. He disclosed to an opposition Member of Parliament documents showing the government's attempt to conceal the fact that during the Falklands conflict, the Argentine ship "General Belgrano" had been sailing away from, and not into, the restricted naval zone established by the British around the Falkland Islands at the time when it was torpedoed.

Ponting maintained in his defence that he had a right to prevent Parliament from being seriously misled by the government. He justified his actions

[144] Sir Lionel Heald QC in *The Times*, 20 March 1970, quoted in DGT Williams, "Official Secrecy and the Courts" in *Reshaping the Criminal Law* (PR Glazebrook, ed, 1978). See also *R* v *Crisp and Homewood, supra*, note 10; Franks Committee Report, *supra*, note 4.

[145] *Supra*, note 112. See also Drewry, "The Ponting Case – Leaking in the Public Interest", *supra*, note 112; Clive Ponting, *The Right to Know* (1985).

on the basis that he believed that he was being required to assist Ministers in their efforts to evade, through deceit, legitimate Parliamentary scrutiny.

The judge directed the jury that section 2(1) of the (UK) Official Secrets Act 1911 is concerned with the preservation of information which had been obtained by virtue of his position as servant of Her Majesty and that the only *mens rea* requirement is an intention to commit the *actus reus*. The prosecution did not have to show that the defendant did not reasonably and honestly believe that the communication was in the interest of the State. Yet, the jury acquitted Ponting of the charge, implicitly accepting a public interest defence when, according to the directions of the judge, none existed at all in the law.

Finally, prosecution for the disclosure of harmless information does not make for good government since it can lead to the protection of inefficiency and malpractice. A comparison may be made with the Civil Service Reform Act 1978 in the United States which gives protection to "whistle-blowers" from administrative discipline.[146] This law protects civil servants who disclose information which they reasonably believe evidences violation of the law or regulations, gross mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety.

It is submitted that the beginnings of an analysis of the issues from a harm perspective can be detected locally. This clarifies the scope of the offence immensely and should be further developed by our courts. Carrying the above analysis through, information which is publicly available is not protected under the Act, not on the basis of the Court of Appeal's reasons, but on the basis that communication of such information cannot cause harm to the interests of the State. However, bearing in mind the criticisms expressed earlier, the fact that the information is publicly available does not necessarily mean that the information cannot cause serious harm from a subsequent publication.

XIV. Conclusion

The Government has indicated that it is dissatisfied with the judicial interpretation given to the scope of the offence. The Minister for Law announced in Parliament that the Government intends to amend the Official Secrets Act.[147] From the recent cases on the Act, it can be seen that the judiciary has been up to the task of regulating the scope of section 5 of the Act to workable

[146] 5 US Code, s 2302.
[147] "Changes may be made: Jayakumar" *The Straits Times*, 15 January 1998.

limits and balancing the concerns of efficient administration and public access to information. The range of information covered by the section and the circumstances in which persons are liable to criminal prosecution are clearer. There is great danger that the Government may brush these developments aside and succumb to the temptation of seeking to widen the scope of criminal liability unnecessarily and defining what is protected information by executive *fiat*. That would be retrogressive.

In the 1988 UK White Paper, it was acknowledged that:

> ...those areas in which disclosure of at least some information may be sufficiently harmful to the public interest to justify the application of criminal sanctions ... is in fact small. For the most part, even if disclosure may obstruct sensible and equitable administration, cause local damage to individuals or groups or result in political embarrassment, it does not impinge on any wider public interest to a degree which would justify applying criminal sanctions.[148]

To this end, the (UK) Official Secrets Act 1989 had identified 5 categories of information in which the public interest in non-disclosure justifies the use of the general official secrets legislation: (1) security and intelligence; (2) defence; (3) international relations and information obtained in confidence from other governments or international organisations; and (5) information useful to criminals.

Outside of these areas, civil servants are subject to disciplinary sanctions for unauthorised disclosures of information, and the civil law of confidence may also be utilised by the Government to prevent disclosures.

As mentioned earlier, there exist many specific offences created for disclosure of information provided by the public to government departments.[149] It should also be noted that the UK Government specifically excluded from protection as a class under their new (UK) Official Secrets Act 1989 the disclosure of Cabinet documents, advice to Ministers and economic information.[150]

Moreover, the idea behind this form of legislation is that all official

[148] 1988 UK White Paper, *supra*, note 7, para 24. See also Franks Committee Report, *supra*, note 4, para 91 and para 4 of the Memorandum submitted by the then Attorney-General to the Franks Committee.

[149] *Supra*, note 63.

[150] 1988 UK White Paper, *supra*, note 7, paras 32, 33. See also the proposal by the Franks Committee to give only limited protection to information relating to currency, Franks Committee Report, *supra*, note 4, paras 135-138.

[151] William Birtles, "Big Brother Knows Best" [1973] PL 100, 119.

information is the property of the State and therefore privileged such that those who receive it may not divulge it without the State's authority[151] is outmoded. It simply fails to recognise the right of citizens to have access to information over the whole range of government activity.

A proper appraisal of secrecy of official information within in a democracy must be made. Greater availability of information fosters participatory democracy by the citizenry and promotes public accountability of government functions.[152] This is relevant in two respects to the protection of information under the Act. First, it places a limitation on the information which can be kept from the public; and secondly, it instructs us as to the proper scope of the defence of "any person ... to whom it is his duty to communicate [the information]".

Finally, openness in government has two aspects. Section 5 of the Official Secrets Act only deals with criminal sanctions against a person who either communicates or receives protected information. It is negative in nature and aims to prevent leaks of information. The other aspect imposes a positive legal obligation on the government to supply information when asked for by the individual. This assumes that access to information is desirable, except in closely specified cases.[153] These two aspects are closely linked. As was opined in a commentary on the *Ponting* case:

> If private conscience is forbidden any overt expression, it may express itself through covert channels. Ultimately, the only credible remedy against illicit leaking is to extend greatly the openness of government and the legitimate outflow of information from departments.[154]

While there are no local legislative movements towards the second aspect of openness, the limitations on the scope of the offence in section 5 of

[152] Sultan Azlan Shah, "The Right to Know" [1986] JMCL 1, 2-3, 9-10; *SP Gupta* v *Union of India* (1981) Supp SCC 87, 275; *LK Koolwal* v *State of Rajasthan* AIR 1988 Raj 2, 4.

[153] For examples of such legislation from other countries, see Freedom of Information Act 1967 (US); Access to Information Act 1982 (Canada); Freedom of Information Act 1982 (Australia); Official Information Act 1982 (New Zealand). See also the latest proposal of the UK Government to enact a Freedom of Information Act, *Your Right to Know* (Cm 3818, 1997). The very first line of this White Paper states: "Unnecessary secrecy in government leads to arrogance in governance and defective decision-making."

[154] Gavin Drewry, "The Ponting Case – Leaking in the Public Interest", *supra*, note 112, at 212.

[155] Prosecutions under the Act may only be made with the consent of the Attorney-General, s 14 Official Secrets Act (Cap 213, 1985 Rev Ed). The cases of *Lim Kit Siang* and *Datuk Haji Dzulkifli* were described as the first two cases ever brought before the court under the Act in Malaysia, *Datuk Haji Dzulkifli, supra*, note 59, at 114.

the Act formulated in recent cases are much welcomed. Although the number of individuals prosecuted under the Official Secrets Act may not be large,[155] its force in shaping the attitudes towards secrecy of official information generally should not be underestimated.[156] The recent judicial developments may yet augur well for open government.[157]

CHAN WING CHEONG*

[156] Anecdotal evidence is provided by Mr Jeyaratnam in *Singapore Parliamentary Debates, Official Reports*, 20 December 1983, cols 221-222.

[157] The need for open government cannot be over-emphasised. In a survey reported in June 1998, Alison de Souza, "8 in 10 have faith in Govt" and "More say in policies, please" *The Straits Times* 20 June 1998, it was found that only 22% of respondents agreed with the statement "The Government consults me on policies affecting me". In a 1989 survey, it was reported that 44% of the respondents felt that they have less influence on national issues than they think they should have, Chiew Seen Kong, "National Identity, Ethnicity and National Issues" in *In Search of Singapore's National Values* (Jon ST Quah ed, 1990), Ch 5. The degree of political alienation is perceived more strongly among those who are younger, with tertiary education, and among Malays and Indians. See also Leslie Koh, "The young and educated more vocal" *The Straits Times* 25 August 1998.

* MA (Oxon); LLM (Cornell); Barrister (GI); Attorney and Counsellor-at-Law (New York State); Advocate & Solicitor (Singapore); Assistant Professor, Faculty of Law, National University of Singapore. I wish to thank Associate Professor Michael Hor for his comments on an earlier draft of this article.

APPENDIX

SECTION 5 OFFICIAL SECRETS ACT (CAP 213, 1985 REV ED) (SINGAPORE)

(1) If any person having in his possession or control any secret official code word, countersign or password, or any photograph, drawing, plan, model, article, note, document or information which –

(a) relates to or is used in a prohibited place or anything in such a place;

(b) relates to munitions of war;

(c) has been made or obtained in contravention of this Act;

(d) has been entrusted in confidence to him by any person holding office under the Government; or

(e) he has obtained, or to which he has had access, owing to his position as a person who holds or has held office under the Government, or as a person who holds, or has held a contract made on behalf of the Government, or as a person who is or has been employed under a person who holds or has held such an office or contract,

does any of the following:

(i) communicates directly or indirectly any such information or thing as aforesaid to any foreign Power other than a foreign Power to whom he is duly authorised to communicate it, or to any person other than a person to whom he is authorised to communicate it or to whom it is his duty to communicate it;

(ii) uses any such information or thing as aforesaid for the benefit of any foreign Power other than a foreign Power for whose benefit he is authorised to use it, or in any manner prejudicial to the safety or interests of Singapore;

(iii) retains in his possession or control any such thing as aforesaid when he has no right to retain it, or when it is contrary to his duty to retain it, or fails to comply with all lawful directions issued by lawful authority with regard to the return or disposal thereof; or

(iv) fails to take reasonable care of, or so conducts himself as to endanger the safety or secrecy of, any such information or thing as aforesaid,

that person shall be guilty of an offence.

(2) If any person receives any secret official code word, countersign, password, or any photograph, drawing, plan, model, article, note, document or information knowing, or having reasonable ground to believe, at the time when he receives it, that the code word, countersign, password, photograph, drawing, plan, model, article, note, document or information is communicated to him in contravention of this Act, he shall be guilty of an offence unless he proves that the communication to him of the code word, countersign, password, photograph, drawing, plan, model, article, note, document or information was contrary to his desire.

...

SECTION 2 OFFICIAL SECRETS ACT 1911 (UK) (BEFORE REPEAL)

2.—(1) If any person having in his possession or control any secret official code word, or pass word, or any sketch, plan, model, article, note, document or information which relates to or is used in a prohibited place or anything in such a place, or which has been made or obtained in contravention of this Act, or which has been entrusted in confidence to him by any person holding office under Her Majesty or which he has obtained, or to which he has had access, owing to his position as a person who holds or has held office under Her Majesty, or as a person who holds, or has held a contract made on behalf of Her Majesty or as a person who is or has been employed under a person who holds or has held such an office or contract –

(a) communicates the code word, or pass word, or any sketch, plan, model, article, note, document or information to any person, other than a person to whom he is authorised to communicate it, or a person to whom it is in the interest of the State his duty to communicate it; or

(aa) uses the information in his possession for the benefit of any foreign Power or in any manner prejudicial to the safety or interests of the State; or

(b) retains the sketch, plan, model, article, note or document in his possession or control when he has no right to retain it or when

it is contrary to his duty to retain it, or fails to comply with all directions issued by lawful authority with regard to the return or disposal thereof; or

(c) fails to take reasonable care of, or so conducts himself as to endanger the safety of the sketch, plan, model, article, note, document, secret official code or pass word or information;

that person shall be guilty of a misdemeanour.

(1A) If any person having in his possession or control any sketch, plan, model, article, note, document or information which related to munitions of war, communicates it directly or indirectly to any foreign Power, or in any manner prejudicial to the safety of interests of the State, that person shall be guilty of a misdemeanour.

(2) If any person receives any secret official code word, or pass word, or sketch, plan, model, article, note, document or information, knowing, or having reasonable ground to believe, at the time when he receives it, that the code word, pass word, sketch, plan, model, article, note, document or information is communicated to him in contravention of this Act, he shall be guilty of a misdemeanour, unless he proves that the communication to him of the code word, pass word, sketch, plan, model, article, note, document or information was contrary to his desire.