Law Commission
Reforming the law

Protection of Official Data
A Consultation Paper

Consultation Paper No 230

Law Commission

Consultation Paper No 230

PROTECTION OF OFFICIAL DATA

A Consultation Paper

This publication is available at www.lawcom.gov.uk.

THE LAW COMMISSION – HOW WE CONSULT

About the Law Commission: The Law Commission was set up by section 1 of the Law Commissions Act 1965 for the purpose of promoting the reform of the law.

The Law Commissioners are: The Rt Hon Lord Justice Bean, *Chairman,* Professor Nicholas Hopkins, Stephen Lewis, Professor David Ormerod QC, Nicholas Paines QC. The Chief Executive is Phillip Golding.

Topic of this consultation: Protection of Official Data. This consultation paper does the following:

- examines the criminal law provisions that protect official data;
- assesses the extent to which the current law could be improved and
- makes a number of provisional conclusions and asks a number of consultation questions.

Geographical scope: This consultation paper applies to the law of England and Wales.

Availability of materials: The consultation paper is available on our website at http://www.lawcom.gov.uk/project/protection-of-official-data/.

Duration of the consultation: We invite responses from 1 February 2017 to 3 April 2017.

Comments may be sent:

By email to pod@lawcommission.gsi.gov.uk

OR

By post to Criminal Law Team, Law Commission, 1st Floor, Tower, 52 Queen Anne's Gate, London, SW1H 9AG.

Tel: 020 3334 3100 / Fax: 020 3334 0201

If you send your comments by post, it would be helpful if, whenever possible, you could also send them electronically (for example, on CD or by email to the above address, in any commonly used format).

After the consultation: In the light of the responses we receive, we will decide on our final recommendations and present them to Government.

Consultation Principles: The Law Commission follows the Consultation Principles set out by the Cabinet Office, which provide guidance on type and scale of consultation, duration, timing, accessibility and transparency.

The Principles are available on the Cabinet Office website at: https://www.gov.uk/government/publications/consultation-principles-guidance.

Information provided to the Law Commission

We may publish or disclose information you provide us in response to this consultation, including personal information. For example, we may publish an extract of your response in Law Commission publications, or publish the response in its entirety. We may also be required to disclose the information, such as in accordance with the Freedom of Information Act 2000.

If you want information that you provide to be treated as confidential please contact us first, but we cannot give an assurance that confidentiality can be maintained in all circumstances. An automatic disclaimer generated by your IT system will not be regarded as binding on the Law Commission.

The Law Commission will process your personal data in accordance with the Data Protection Act 1998.

THE LAW COMMISSION

PROTECTION OF OFFICIAL DATA
A CONSULTATION PAPER

CONTENTS

CHAPTER 1
INTRODUCTION

INTRODUCTION

1.1 Technological advances have increased the ability of government to deal with large amounts of information, which has had a significant impact upon the relationship between citizens and government. Terrill has argued that information now "underpins almost all government activity" and it is both "an object in its own right" in addition to being "a dimension of all government activity."[1]

1.2 The focus of this project is on the effectiveness of those criminal law provisions that protect official information. It is important at this stage to point out that not all information held by government is protected by the criminal law. As subsequent chapters will demonstrate, criminalisation is limited to the unauthorised disclosure of those categories of information that have implications for the national interest. It also limited to those working within or alongside government who have been trained in how to handle sensitive information.

1.3 The project is not limited to those provisions that criminalise those who, being lawfully in possession of official information, disclose it without authorisation. The project also includes those provisions that criminalise individuals whose purpose is to gain access to information, potentially by using covert means. This is sometimes referred to as espionage.

1.4 The key offences that protect official information are primarily contained in the Official Secrets Acts 1911-1989. As subsequent chapters will demonstrate, this legislation has been subject to very little scrutiny in the past. The present review is the first occasion in the century since the Official Secrets Act 1911 was enacted that it has been subject to sustained, holistic, independent scrutiny. The same is true of the Official Secrets Act 1989. This review therefore presents a rare opportunity.

THE PROJECT

1.5 The Protection of Official Data project was referred to us by the Cabinet Office in late 2015. We commenced work on the project in February 2016 and plan to publish our final report in Spring 2017.

1.6 We agreed the following terms of reference with the Cabinet Office:

(1) The Review will examine the effectiveness of the criminal law provisions that protect Government information from unauthorised disclosure. The Review will assess any deficiencies in the law, and research options for improving the protection of official information with the aim of providing an effective and coherent legal response to unauthorised disclosures. The Review will also examine provisions that criminalise those who illegitimately obtain or attempt to obtain official information.

[1] G Terrill, *Secrecy and Openness: The Federal Government from Menzies to Whitlam and Beyond* (2000) pp 3-5. These comments were made in the context of the Australian state, but we believe they are equally applicable to the domestic context.

(2) The review will include, but will not be limited to, the Official Secrets Acts 1911, 1920 and 1989. It will want to consider other criminal provisions that protect information held by Government from unauthorised disclosure and to take into account relevant aspects of the Data Protection Act 1998, the Public Interest Disclosure Act 1998 and the protections for information exempt from release under the Freedom of Information Act 2000. The Review will take a holistic approach and examine how the legislative landscape could be rationalised and made more coherent.

(3) The Review will also consider:

(a) the relationship between the legislative regime and internal disciplinary measures to which public servants and others are subject;

(b) the powers available to investigators;

(c) the relationship between the criminal law and any civil remedies;

(d) the effect of technological change on the way in which data is stored, shared and understood, and determine whether the current law needs to be reformed properly to account for these changes.

LEGAL CONTEXT

1.7 Our terms of reference mandate that we are to consider the extent to which the relevant legislation effectively protects official information. Whilst this has been our focus, we have also sought to assess the extent to which the legislation strikes an appropriate balance between transparency and secrecy. Given that the relevant legislation was enacted long before the Human Rights Act 1998 came into force, we have also sought to assess the extent to which the relevant provisions comply with the European Convention on Human Rights.

1.8 As subsequent chapters will discuss, we have provisionally concluded that there are ways the legislation could be improved both to ensure that it protects information more effectively and ensures greater compliance with the European Convention on Human Rights. Our provisional conclusions in relation to how the legislation could be improved have been informed by the initial consultation we have conducted with a broad range of stakeholders. A list of the departments, practitioners and organisations we have consulted with is contained in Appendix B.

1.9 A fundamental aspect of our review of the relevant legislation is the fact that we are conducting an open, public consultation. We believe this is crucial to ensuring public confidence in our provisional conclusions. With that in mind, we are keen to know from consultees whether they agree that we have identified the most pressing problems with the legislation, and whether they agree with our provisional conclusions as to how they could be remedied.

1.10 We are aware of the existence of those who disagree with the proposition that the unauthorised disclosure of information should be criminalised. Our terms of reference did not permit us to question this underlying assumption. We do firmly believe, however, that certain categories of information require the effective protection of the criminal law and that it is necessary to ensure sensitive information is safeguarded against those whose goal is to obtain it contrary to the national interest.

THE WAY WE HAVE WORKED

1.11 Our research methodology in preparing this paper was twofold. First, we undertook a review of relevant literature, including legislation, case-law, policy papers, government papers and academic work. Furthermore, we commissioned a review of the relevant legal provisions in five other English speaking jurisdictions. This research is contained in Appendix A.

1.12 Secondly, as we have already discussed, we engaged in preliminary consultation with various government departments, non-governmental organisations and practitioners. A list of the departments, practitioners and organisations that we have engaged with is set out in Appendix B.

THE SCHEME OF THIS PAPER

1.13 This consultation paper is structured as follows:

(1) Chapter 1 is this introduction.

(2) Chapter 2 examines the Official Secrets Acts 1911, 1920 and 1939.

(3) Chapter 3 examines the Official Secrets Act 1989.

(4) Chapter 4 examines the miscellaneous unauthorised disclosure offences our research has uncovered.

(5) Chapter 5 discusses the procedural matters related to prosecutions and investigations under the Official Secrets Acts.

(6) Chapter 6 examines the compatibility of unauthorised disclosure offences with freedom of expression. It focuses particularly on the Official Secrets Act 1989.

(7) Chapter 7 assesses the case that could be made for introducing a statutory public interest defence to the unauthorised disclosure offences examined in this paper. Alternative models which would allow for consideration of the public interest are also assessed.

(8) Chapter 8 lists our provisional proposals and consultation questions.

(9) Appendix A sets out the relevant law from five other English speaking jurisdictions.

(10) Appendix B contains a list of the departments, organisations and practitioners that we have met and whose views have informed our provisional conclusions and consultation questions.

(11) Appendix C contains a list of the miscellaneous unauthorised disclosure offences that our research has uncovered.

(12) Appendix D sets out the Official Secrets Acts 1911-1989 to aid consultees' comprehension of our provisional conclusions and consultation questions.

CHAPTER 2
THE OFFICIAL SECRETS ACTS 1911, 1920 AND 1939

INTRODUCTION

2.1 This chapter analyses the provisions contained in the Official Secrets Acts 1911, 1920, and 1939. These need to be read together to understand the full picture of legislative protection. It is expedient to consider these three pieces of legislation in the same chapter, because the Official Secrets Act 1920 amends the Official Secrets Act 1911, while the Official Secrets Act 1939 amends the Official Secrets Act 1920. The Official Secrets Act 1920 also contains freestanding provisions. Section 2 of the Official Secrets Act 1911 was repealed by the Official Secrets Act 1989 and will be considered in Chapter 3.

2.2 The Official Secrets Acts 1911-1939 are broadly concerned with espionage. According to the MI5 website, "espionage" is:

> The process of obtaining information that is not normally publicly available, using human sources (agents) or technical means (like hacking into computer systems). It may also involve seeking to influence decision-makers and opinion-formers to benefit the interests of a foreign power.[1]

2.3 The MI5 website goes on to give the following reasons for why espionage is damaging:

> Espionage focuses on gathering non-public information through covert means. Classified information is kept secret in the first place because its disclosure might harm national security, jeopardise the country's economic well-being or damage international relations. Its sensitivity makes it necessary for us to protect it but also makes it attractive to spies.
>
> If this information is obtained by those with no right to access it, serious damage can be caused. For instance, other countries are seeking technical details of weapons systems so that they can find ways of neutralising our military advantages. Information on key services such as gas, oil and transport could enable terrorists to seriously damage these important economic targets. And the theft of

[1] https://www.mi5.gov.uk/espionage (last visited 9 November 2016).

classified technologies could enable foreign companies to copy them, threatening both national security and jobs in the UK.[2]

2.4 Given the potential damage such activity can cause to the national interest, it is crucial that the United Kingdom has a robust legislative response that meets the challenges posed by espionage in the 21st century. This chapter examines the extent to which the current legislative regime meets these challenges.

2.5 At this stage, it is important to point out that the Official Secrets Acts 1911 - 1939 are not the only legislative provisions that criminalise espionage related activity. The Computer Misuse Act 1990 criminalises a number of forms of activity that could be linked to espionage.[3] Although there are no specific offences that criminalise the misuse of a computer for the purposes of espionage, the offences of general application are sufficiently capacious to criminalise such behaviour. Given the nature of the activity in question, it could be difficult for the prosecution to prove that the defendant was misusing a computer for the purposes of espionage, so the fact that the legislation does not specify that there must be a link to espionage could be considered advantageous. Section 1 of the Computer Misuse Act 1990 makes it an offence to access computer material without authorisation. An aggravated form of this offence is created by section 2 if a person commits an offence under section 1 with intent to commit or facilitate the commission of further offences.

2.6 Section 3 makes it an offence for a person to do an unauthorised act in relation to a computer with intent to impair, or being reckless as to whether he or she would impair the operation of any computer, would prevent or hinder access to any programme or data held in any computer, would impair the operation of any such programme or the reliability of any such data, or would enable any of these things to be done.

2.7 By virtue of section 3ZA, a person commits an offence if he or she does any unauthorised act in relation to a computer, the act causes or creates a significant risk of causing, serious damage of a material kind and the person intends by doing the act to cause serious damage of a material kind or is reckless as to whether such damage is caused.[4] Damage is of a "material kind" if it causes damage to human welfare in any place, damage to the environment of any place, damage to the economy of any country, or damage to the national security of any country. If the act in question causes or creates a significant risk of causing

[2] https://www.mi5.gov.uk/espionage (last visited 9 November 2016).

[3] For discussion of these offences, see D Ormerod and D Perry (eds), *Blackstone's Criminal Practice* (2017) para B17.

[4] This provision was inserted by Part 2 of the Serious Crime Act 2015.

serious damage to human welfare or serious damage to national security, then the offence carries a maximum sentence of life imprisonment.

2.8 In addition to the offences that are contained in the Computer Misuse Act 1990, section 58 of the Terrorism Act 2000 makes it an offence to collect or make a record of information of a kind likely to be useful to a person committing or preparing an act of terrorism, or to possess a document or record containing information of that kind.

BACKGROUND

2.9 The Official Secrets Act 1911 still provides the principal legal protection in the United Kingdom against espionage. Espionage differs from the types of unauthorised disclosure that are discussed in Chapter 3, as espionage not only encompasses the unauthorised disclosure of information, but also the process of obtaining information that is not publicly available.

2.10 During the late nineteenth century, the United Kingdom experienced outbreaks of both unauthorised disclosures and espionage.[5] These were the catalyst for the enactment of the Official Secrets Act 1889. The Bill of 1889 was introduced into the House of Commons by the then Attorney General and contained numerous provisions that criminalised both espionage and unauthorised disclosures. The Official Secrets Act 1889 was criticised on the basis that it imposed a difficult burden on the prosecution and contained inadequate enforcement powers.

2.11 Thomas describes how, by 1909, there was increasing alarm in the United Kingdom caused by the perception that German spies were operating within the country.[6] A sub-committee of the Committee on Imperial Defence was established to examine the extent of this problem. One of the recommendations made by the Committee was the strengthening of the provisions contained in the Official Secrets Act 1889. The Committee also recommended that these provisions should be given effect in a new Act. To this end, it was further recommended that the requisite Bill should be introduced by the Secretary of State for War as a "national defence" precaution, rather than by the Home Secretary or the Attorney General. This task ultimately fell to Viscount Haldane, the then Secretary of State for War.[7]

2.12 The Official Secrets Bill was introduced into the House of Lords on 17 July 1911 and received the Royal Assent on 22 August 1911. It was therefore subject to

[5] R Thomas, *Espionage and Secrecy* (1991) p 3. For detailed analysis of the history of the legislation, see D Williams, *Not in the Public Interest* (1965).

[6] R Thomas, *Espionage and Secrecy* (1991) p 12.

[7] *Hansard* (HL), 25 July 1911, vol 9, cc 641-647.

very little scrutiny by Parliament. The Bill's expedited passage was described in Parliament as "distressing" and "undesirable".[8]

2.13 The following sections of this chapter will analyse the key provisions of the legislation as amended. Section 2 of the Official Secrets Act 1911, which criminalises the wrongful communication of information, was repealed and replaced by the Official Secrets Act 1989, which will be discussed in Chapter 3.

SECTION 1 – 'PENALTIES FOR SPYING'

2.14 Although the terms "espionage" or "spying" are not used in section 1 of the Official Secrets Act 1911, Viscount Haldane did use the former term when introducing the Official Secrets Bill in the House of Lords.[9]

2.15 Before examining in detail the provisions in section 1, it is necessary to examine what they replaced. In 1911 Viscount Haldane, whilst accepting that the changes to the espionage offences introduced by the Official Secrets Act 1911 were significant, stated that they were mostly procedural in nature. To secure a conviction under the 1889 Act the prosecution had to prove that the defendant acted with "a purpose of wrongfully obtaining information." According to Thomas, in practice proof of such a purpose proved very difficult for the prosecution to obtain, which led to prosecutions of suspected spies not being instituted.[10]

2.16 The main aim of the Official Secrets Act 1911 was therefore to relieve the prosecution of the burden of proving that the defendant acted with a purpose of wrongfully obtaining information and to alter the focus of the offences to include situations where the defendant acted with "any purpose prejudicial to the safety or interests of the state".

THE OFFENCES

2.17 Section 1 of the Official Secrets Act 1911 creates three distinct offences:

(1) Section 1(1)(a) – makes it an offence for a person, for any purpose prejudicial to the safety or interests of the state to approach, inspect, pass over, be in the neighbourhood of, or enter any prohibited place as that term is defined in the Act.

(2) Section 1(1)(b) – makes it an offence for a person for any purpose prejudicial to the safety or interests of the state to make any sketch, plan,

[8] *Hansard* (HL), 18 August 1911, vol 29, cc 2257.

[9] *Hansard* (HL), 25 July 1911, vol 9, cc 642.

[10] R Thomas, *Espionage and Secrecy* (1991) p 6.

model or note which is calculated to be, or might be, or is intended to be directly or indirectly useful to an enemy.

(3) Section 1(1)(c) – makes it an offence for a person for any purpose prejudicial to the safety or interests of the state to obtain, collect, record, publish, or communicate to any other person, any secret official code word, or pass word, or any sketch, plan, model, article, note, or other document or information which is calculated to be, or might be or is intended to be directly or indirectly useful to an enemy.

2.18 By virtue of section 8(1) of the Official Secrets Act 1920, these offences can only be tried in the Crown Court and carry a maximum sentence of 14 years' imprisonment.[11]

2.19 The conduct elements of each of these offences are relatively clear, albeit archaic in their drafting. In section 1(1)(a) the conduct that is proscribed is "approaching, inspecting, passing over, being in the neighbourhood of, or entering". In section 1(1)(b) it is making any sketch, plan, model or note. In section 1(1)(c) it is obtaining, collecting, recording, publishing, or communicating to any other person, any secret official code word, or pass word, or any sketch, plan, model, article, note, or other document or information. The conduct elements are very broad and are clearly drafted so as to minimise the risk that none of those forms of espionage that would be typical of the era were omitted.

2.20 Although the conduct elements of the offences are clear, there are however a number of ambiguities within section 1(1) that have been considered by the courts in the decades since the Official Secrets Act 1911 was enacted. These will be analysed in the following sections.

2.21 In this chapter, we can begin by examining aspects that are common to all of the offences:

(1) are the offences limited to spying;

(2) what is the meaning of the expression "purpose prejudicial";

(3) the meaning of the expression "safety or interests of the state".

2.22 We then examine those issues that only apply to specific offences:

[11] In *Devenney* (12 December 2012) (unreported) Mr Justice Saunders handed down a sentence of 8 years' imprisonment and considered that a deterrent sentence was required even though the defendant had achieved nothing by his actions. See D Ormerod and D Perry (eds), *Blackstone's Criminal Practice* (2017) para B9.4.

(1) the concept of "enemy" which applies in relation to section 1(1)(b) and section 1(1)(c);

(2) the concept of prohibited place that applies to section 1(1)(a)

The scope of the offences in section 1

2.23 In the middle of the 20th century, a fundamental issue arose as to the scope of the Act, namely whether section 1 was confined to spying or whether it encompassed other forms of behaviour.[12] The marginal note to section 1 reads, "penalties for spying", which lends weight to the suggestion that it was intended only to encompass spying.

2.24 In *Chandler and others v Director of Public Prosecutions,* however, the House of Lords rejected the reliance placed by the defendants on the marginal note and concluded that section 1 was sufficiently broad to encompass acts of sabotage to an airfield.[13] The appellants were members of an organisation that sought to further the aims of the Campaign for Nuclear Disarmament by non-violent civil disobedience. They took part in a demonstration at Wethersfield Airfield, which was a prohibited place within the meaning of section 3 of the Official Secrets Act 1911. The aim of the appellants was to immobilise the base and reclaim it for civilian purposes. They were charged with conspiring together and inciting persons to commit offences contrary to the Official Secrets Act 1911.

2.25 The House of Lords held that the use of the terms "damage", "destruction" and "obstruction" in section 3(c) and section 3(d) of the Official Secrets Act 1911 suggested Parliament did intend for section 1(1) of the 1911 Act to encompass acts of sabotage, in addition to acts of spying. This makes the offences broader than they might at first appear. In this regard, section 3 supports the conclusion of the House of Lords by providing that one basis for designating a place "a prohibited place" is that information in respect of that place, the destruction or obstruction of that place, or interference with that place, would be useful to an enemy.

The meaning of the phrase "purpose prejudicial"

2.26 The meaning of this key phrase was also considered by the House of Lords in *Chandler and others v Director of Public Prosecutions.*[14] The appellants appealed to the House of Lords on the basis that they did not have a purpose prejudicial to

[12] R Thomas, *Espionage and Secrecy* (1991) pp 35-36.

[13] *Chandler and others v Director of Public Prosecutions* [1964] AC 763; [1962] 3 WLR 694.

[14] For further discussion, see J C Smith and B Hogan, *Criminal Law* (6th ed 1988) pp 839-840.

the interests of the state because they believed it was in the interests of the state that the aircraft stationed at the base, which they believed to contain nuclear weapons, should be immobilised.

2.27 The House of Lords rejected this argument and made the following observations:

(1) The term "purpose" imports a subjective element. To be guilty of the offence in section 1(1) of the Official Secrets Act 1911, it must be proved that the defendant, when he or she acted, knew that certain objects "will probably be achieved by the act, whether he wants them to or not."[15] On the facts of *Chandler*, it was sufficient to prove that the defendants entered the air base with the purpose of immobilising it.

(2) Once it was proved that the defendants' purpose was to immobilise the airbase, the further question of whether that purpose was prejudicial to the safety or interests of the state was an objective one. Therefore, the defendants' opinion as to whether that was beneficial or prejudicial to the interests of the state was irrelevant.

(3) Whether the Crown's policy regarding nuclear weapons was right or wrong was similarly irrelevant and no evidence could be called that went to this issue.[16] The House of Lords held that such matters were the exclusive discretion of the Crown and were not capable of being tried in a court. Lord Hodson and Lord Devlin cited with approval the following statement earlier made by Lord Parker in *The Zamora*:

> Those who are responsible for the national security must be the sole judges of what the national security requires.[17]

2.28 Although the decision has been vigorously criticised, [18] in their analysis of the case, Professors Smith and Hogan argued that the House of Lords arrived at the only sensible interpretation of the Act. They elaborated as follows:

> If it were necessary to prove that D believed his object to be prejudicial to the interests of the State, a man would have had a

[15] *Chandler and others v Director of Public Prosecutions* [1964] AC 763; [1962] 3 WLR 694, 805, by Lord Devlin.

[16] In the subsequent case of *Bettaney* (1985) *Criminal Law Review* 104, the court confirmed that the opinion of the defendant as to what is in the best interests of the state is irrelevant. See D Ormerod and D Perry (eds), *Blackstone's Criminal Practice* (2017), at B9.6.

[17] *The Zamora* [1916] 2 AC 77, 107.

[18] D Thompson, "The Committee of 100 and the Official Secrets Act 1911" (1963) *Public Law* 201.

> defence if, during the world wars, he believed that it was in Britain's interests that Germany should win the war. Such an interpretation would obviously defeat the object of the Act. If the question were whether the policy of the Crown which D obstructed was in the interests on the state, the court would be presented with an issue which it could not properly try; and if the Act can reasonably be read so as to avoid raising such an issue, then it should be so read.[19]

The meaning of the phrase "the safety or interests of the state"

2.29 In *Chandler and others v Director of Public Prosecutions* the House of Lords also considered how the phrase "safety or interests of the state" ought to be interpreted. The Court concluded that this phrase means the objects of state policy determined by the Crown on the advice of Ministers.

2.30 Thomas argues that the framers of the Official Secrets Act 1911 assumed without question that it is the responsibility of the Crown to determine what is in the safety and interests of the state.[20] As we have explained, this assumption was challenged by the defendants in *Chandler and others v Director of Public Prosecutions*, as they sought to adduce evidence that their ultimate purpose in disrupting the United Kingdom's ability to arm itself with nuclear weapons would benefit the United Kingdom. Their argument was that the presence of nuclear weapons in the United Kingdom would increase the risk of nuclear retaliation and it was therefore in the interest of the state to minimise this possibility by not having nuclear weapons present in the United Kingdom. The judgment of the House of Lords means that such evidence would be irrelevant and therefore inadmissible.

2.31 A variety of interpretations as to how the phrase "the safety or interests of the state" ought to be interpreted were proffered by the Law Lords. Lord Reid treated the word "state" as being synonymous with "the realm" whilst Lord Hodson preferred the term "the organised community".[21] Lord Devlin suggested "the organs of government of a national community".[22]

2.32 In relation to the phrase, "interests of the state", Lord Devlin held that the focus of the statute is on "the interests of the state at the time of the alleged offence" rather than on what those interests might be or ought to be. Importantly, Lord

[19] J C Smith and B Hogan, *Criminal Law* (6th ed, 1988) pp 840-841.

[20] R Thomas, *Espionage and Secrecy* (1991) p 45.

[21] *Chandler and others v Director of Public Prosecutions* [1964] AC 763; [1962] 3 WLR 694, 790, by Lord Reid and 801, by Lord Hodson.

Devlin considered whether the phrase "interests of the state" ought to be synonymous with "interests of the community". Such an interpretation was rejected on the basis that the legislation was intended to be understood in much narrower terms. He elaborated as follows:

> This statute is concerned with the safety and interests of the State and therefore with the objects of State policy even though judged *sub specie aeternatis*, that policy may be wrong.[23]

2.33 For the purposes of the Official Secrets Act 1911, therefore, the phrase "interests of the state", means the objects of state policy determined by the Crown on the advice of Ministers. Lord Devlin gave examples of absurd consequences that would follow if this element of the offence were given a broader meaning. He stated that:

> Rebels and high-minded spies could be heard to argue that defeat in battle would serve the best interests of the nation because it would be better off under a different regime.[24]

2.34 Lord Reid was less absolute in his judgment and did not believe that the Government's view should always be determinative of what is in the interests of the state.[25] On the facts of the case, however, because the defendants interfered with a prohibited place as defined in the legislation, namely RAF Wethersfield, Lord Reid concluded that what is in the interests of the state was a matter that was best left to be determined by the Government.

The meaning of the phrase "useful to an enemy"

2.35 The term "useful to an enemy" is central to some of the offences in section 1 of the Official Secrets Act 1911. There is uncertainty, however, over how "enemy" ought to be defined in this context. When the Official Secrets Bill was being debated in the House of Lords, the suggestion was made that the term "enemy"

[22] *Chandler and others v Director of Public Prosecutions* [1964] AC 763; [1962] 3 WLR 694, 807.

[23] *Chandler and others v Director of Public Prosecutions* [1964] AC 763; [1962] 3 WLR 694, 808.

[24] *Chandler and others v Director of Public Prosecutions* [1964] AC 763; [1962] 3 WLR 694, 808.

[25] *Chandler and others v Director of Public Prosecutions* [1964] AC 763; [1962] 3 WLR 694, 790.

should be replaced with the term "foreign power".[26] The justification for this amendment was that it would ensure the offences could still be committed in peacetime when no enemies in fact exist.

2.36 The first case to consider the definition of "enemy" was *Parrott*, in which the defendant was charged with "having feloniously communicated to an unknown person at Ostend unspecified information in regard to the arms, armaments, dispositions and movements of ships and men of the Royal Navy which could be useful to an enemy."[27]

2.37 The defendant was convicted and appealed. In dismissing the appeal, Mr Justice Phillimore gave guidance on how the term "enemy" ought to be understood:

> When the statute uses the word "enemy" it does not mean necessarily someone with whom this country is at war, but a potential enemy with whom we might someday be at war.[28]

2.38 Depending upon how this statement is interpreted, it relieves the prosecution of the burden of proving that the country in question was in fact an enemy of the United Kingdom. This is because, hypothetically speaking, the United Kingdom could someday be at war with any country. On the other hand, this statement could be interpreted narrowly, and require the prosecution to place evidence before the jury that there is a realistic possibility that the United Kingdom could someday be at war with the country in question.

2.39 At this stage it is also necessary to point out that the Official Secrets Bill 1920 initially referred to "enemy agent", but this was amended to "foreign power". Both the terms enemy and foreign power are used in the legislation.

SECTION 3 – DEFINITION OF PROHIBITED PLACE

2.40 Section 3 of the Official Secrets Act 1911 sets out an extensive definition of "prohibited place". This definition expands the scope of the offence contained in section 1(1)(a) of the Official Secrets Act 1911, which is why we believe it is necessary to set the definition out in full:

> (a) any work of defence, arsenal, naval or air force establishment or station, factory, dockyard, mine, minefield, camp, ship, or aircraft belonging to or occupied by or on behalf of Her Majesty, or any

[26] *Hansard* (HL), 25 July 1911, vol 9, c 647.

[27] *R v Parrott* (1913) 8 Cr App R 186. Discussed in D Williams, *Not in the Public Interest* (1965) pp 31-32.

[28] *R v Parrott* (1913) 8 Cr App R 186, 192.

telegraph, telephone, wireless or signal station, or office so belonging or occupied, and any place belonging to or occupied by or on behalf of Her Majesty and used for the purpose of building, repairing, making, or storing any munitions of war, or any sketches, plans, models or documents relating thereto, or for the purpose of getting any metals, oil, or minerals of use in time of war;

(b) any place not belonging to Her Majesty where any munitions of war, or any sketches, models, plans; or documents relating thereto, are being made, repaired, gotten, or stored under contract with, or with any person on behalf of, Her Majesty, or otherwise on behalf of Her Majesty; or

(c) any place belonging to or used for the purposes of Her Majesty which is for the time being declared by order of a Secretary of State to be a prohibited place for the purposes of this section on the ground that information with respect thereto, or damage thereto, would by useful to an enemy; and

(d) any railway, road, way, or channel, or other means of communication by land or water (including any works or structures being part thereof or connected (therewith), or any place used for gas, water, or electricity works or other works for purposes of a public character, or any place where any munitions of war, or any sketches, models, plans or documents relating thereto, are being made, repaired, or stored otherwise than on behalf of Her Majesty, which is for the time being declared by order of a Secretary of State to be a prohibited place for the purposes of this section, on the ground that information with respect thereto, or the destruction or obstruction thereof, or interference therewith, would be useful to an enemy.

2.41 It is important to point out that the definition is capable of being expanded, since the Secretary of State can declare a location to be a "prohibited place" for the purposes of the Official Secrets Act 1911. According to our research, this power has been exercised infrequently.[29]

2.42 The definition of "prohibited place" became particularly contentious between the 1960s and the 1980s when the Official Secrets Act 1911 was used to prosecute anti-nuclear demonstrators. For example, Williams questioned whether "the full

[29] See the Official Secrets (Prohibited Place) Order 1955/1497; the Official Secrets (Prohibited Place) Order 1956/1438; the Official Secrets (Prohibited Places) (Amendment) Order 1993/863; the Official Secrets (Prohibited Places) Order 1994/968.

weight of the Official Secrets Act" needed to be used against protesters.[30] Thomas suggests that the enactment of the Public Order Act 1986 led to a decline in the need to invoke the Official Secrets Act 1911 in this context.[31] This would certainly explain why the Official Secrets Act 1911 has not been invoked in this context for a number of years. More recently, the provisions contained in the Serious Organised Crime and Police Act 2005, which are discussed below, could also explain why the Official Secrets Act 1911 is infrequently relied upon in such cases.

Proof of the section 1 offences

2.43 Other provisions in the 1911 Act and the 1920 Act make the proof of these offences easier than might appear from the discussion so far.

The fault element of the offences in section 1

2.44 Section 1(2) of the Official Secrets Act 1911 provides that the prosecution does not need to prove that the defendant did any particular act tending to show a purpose prejudicial to the safety or interests of the state. Notwithstanding that no such act has been proved against him or her, the defendant may be convicted if, from the circumstances of the case, or from the defendant's conduct, or from his or her "known character as proved", it appears that his or her purpose was a purpose prejudicial to the safety or interests of the State. Set out in full, section 1(2) provides as follows:

> On a prosecution under this section, it shall not be necessary to show that the accused person was guilty of any particular act tending to show a purpose prejudicial to the safety or interests of the State, and, notwithstanding that no such act is proved against him, he may be convicted if, from the circumstances of the case, or his conduct, or his known character as proved, it appears that his purpose was a purpose prejudicial to the safety or interests of the State; and if any sketch, plan, model, article, note, document, or information relating to or used in any prohibited place within the meaning of this Act, or anything in such a place or any secret official code word or pass word, is made, obtained, collected, recorded, published, or communicated by any person other than a person acting under lawful authority, it shall be deemed to have been made, obtained, collected, recorded, published or communicated for a purpose prejudicial to the safety or interests of the State unless the contrary is proved.

[30] D Williams, *Not in the Public Interest* (1965) p 111.

[31] R Thomas, *Espionage and Secrecy* (1991) pp 91-92.

2.45 In the Official Secrets Act 1889, the words "knowingly" and "wilfully" were included in the espionage offences. Thomas infers from this that historically fault *was* an element of espionage and related offences. When the Official Secrets Act 1911 re-enacted the Official Secrets Act 1889 with amendments, the phrase "purpose prejudicial to the safety or interests of the state" was introduced.

2.46 The requirement to prove fault is embodied in the "purpose prejudicial" test and is an inherent element of the espionage offence.

2.47 Although there was no mention of fault during the Parliamentary debates that led to the enactment of the Official Secrets Act 1911, Thomas states:

> However, there appears to have been no consideration in 1911 of making the serious crime of espionage an absolute offence in order to surmount the difficulty for the prosecution of proving *mens rea* (fault). Indeed, if an absolute offence had been established, the espionage provisions would be *broader* than at present because the "purpose prejudicial" test narrows the definition of the crime insofar as a person cannot be found guilty unless *intent* to damage the State was present. The alternative solution adopted in 1911 was to shift the burden of proof from the prosecution on to the accused.[32]

2.48 In describing the relevant clauses in the Official Secrets Bill, Viscount Haldane pointed out that under the changed procedure that the 1911 Act would introduce, "the accused has to satisfy the jury that his purpose was a right one", rather than the prosecution being under a burden to prove that his or her purpose was prejudicial.

2.49 Potentially all the prosecution needs to prove, therefore, is that the defendant did an act *or* had such a character that it *appeared* that his or her purpose was to prejudice the safety or interests of the state. The prosecution does not need to prove that the defendant *in fact* had such a purpose.

2.50 For present purposes it suffices to say that the provisions contained in section 1(2) reflect the fact the legislation was intended to ease the evidential difficulties the prosecution encountered when attempting to prosecute suspected spies under the Official Secrets Act 1889.

Presumptions introduced by the Official Secrets Act 1920

2.51 To understand how section 1 operates, it is also necessary to have regard to the relevant provisions contained in the Official Secrets Act 1920.

[32] R Thomas, *Espionage and Secrecy* (1991) p 53.

2.52 By 1920 there was the perception that it was still too difficult to obtain convictions for espionage. This resulted in a second relaxation of the elements the Crown was required to prove was necessary.[33] As such, section 2(1) of the Official Secrets Act provides that:

> In any proceedings against a person for an offence under section one of the [Official Secrets Act 1911], the fact that he has been in communication with, or attempted to communicate with, a foreign agent, whether within or without the United Kingdom, shall be evidence that he has, for a purpose prejudicial to the safety or interests of the State, obtained or attempted to obtain information which is calculated to be or might be or is intended to be directly or indirectly useful to an enemy.

2.53 Furthermore, section 2(2) provides:

> (a) A person shall, unless he proves the contrary, be deemed to have been in communication with a foreign agent if—
>
> (i) He has, either within or without the United Kingdom, visited the address of a foreign agent or consorted or associated with a foreign agent; or
>
> (ii) Either, within or without the United Kingdom, the name or address of, or any other information regarding a foreign agent has been found in his possession, or has been supplied by him to any other person, or has been obtained by him from any other person.

2.54 Section 2(2)(b) defines the term "foreign agent" as follows:

> The expression "foreign agent" includes any person who is or has been or is reasonably suspected of being or having been employed by a foreign power either directly or indirectly for the purpose of committing an act, either within or without the United Kingdom, prejudicial to the safety or interests of the State, or who has or is reasonably suspected of having, either within or without the United Kingdom, committed, or attempted to commit, such an act in the interests of a foreign power.

2.55 Finally, according to section 2(2)(c):

[33] R Thomas, *Espionage and Secrecy* (1991) pp 11-15.

> Any address, whether within or without the United Kingdom, reasonably suspected of being an address used for the receipt of communications intended for a foreign agent, or any address at which a foreign agent resides, or to which he resorts for the purpose of giving or receiving communications, or at which he carries on any business, shall be deemed to be the address of a foreign agent, and communications addressed to such an address to be communications with a foreign agent.

2.56 In *Kent* the trial judge emphasised to the jury that communication with a foreign agent is not conclusive evidence, but it is evidence from which a jury may infer that the defendant acted with a purpose prejudicial to the interests of the state. The Court of Criminal Appeal upheld this direction.[34]

2.57 Prevezer was critical of these provisions on the basis that they left the prosecution with very little to prove.[35] Thomas argues that there were practical reasons for the amendments:

> While this statement is partly true, Prevezer fails to appreciate the situation in Britain which led to the need for this second easement of proof or the continuing difficulty in obtaining evidence in cases of espionage and related crimes. Developments in modern espionage methods made it hard to detect the crime and to gather the evidence. In many cases the only evidence against a person recognised as being a spy was the fact that he had visited or communicated with a known foreign agent. Therefore a further provision was required to facilitate the conviction of spies who for a purpose prejudicial were passing information to an enemy.[36]

2.58 Thomas may be accurate in stating that there were specific problems which existed at the time and which were relied upon to justify the introduction of section 2 of the Official Secrets Act 1920. That does not, however, alter the fact that the amendments leave the prosecution with very little to do in respect of proving some of the offences.

SECTION 7 – OFFENCE OF HARBOURING SPIES

2.59 Section 7 of the Official Secrets Act 1911 creates a number of offences, each carrying a maximum sentence of 2 years' imprisonment if tried in the Crown

[34] *R v Kent* (1943) 28 Cr App R 23. For discussion, see D Ormerod and D Perry (eds), *Blackstone's Criminal Practice* (2017) para B9.9.

[35] S Prevezer, "Peacetime Espionage and the Law" (1953) 6(1) *Current Legal Problems* 88.

[36] R Thomas, *Espionage and Secrecy* (1991) p 57.

Court and 3 months and/or a fine if tried in a magistrates' court. First, it is an offence for a person knowingly to harbour any person whom he or she knows, or has reasonable grounds for supposing, is a person who is about to commit or who has committed an offence contrary to the Official Secrets Act 1911.

2.60 Secondly, it is also an offence for a person knowingly to permit any such persons to meet or assemble in any premises in his or her occupation or under his or her control.

2.61 Finally, it is an offence for any person, having harboured someone who has committed an offence contrary to the Official Secrets Act 1911, or permitted such a person to meet or assemble in any premises in his occupation or under his control, wilfully to omit or refuse to disclose to a superintendent of police any information which it is in his power to give in relation to any such person.

PROCEDURE

2.62 By virtue of section 8 of the Official Secrets Act 1911 a prosecution cannot be commenced except by, or with the consent of, the Attorney General. We examine the Attorney General's role more fully in Chapter 3, when we examine the Official Secrets Act 1989.

2.63 Section 9 gives a justice of the peace the power to issue a search warrant if satisfied that there are reasonable grounds for suspecting that an offence contrary to the Official Secrets Act 1911 has been, or is about to be, committed. The warrant authorises a constable to enter any premises, if necessary by force, to search the premises and every person within them and seize any sketch, plan, model, article, note or document, or anything of a like nature which is evidence of an offence under the Official Secrets Act 1911 having been committed.

2.64 Importantly, section 9(2) of the Official Secrets Act 1911 negates the need to obtain a search warrant from a justice of the peace in certain circumstances. Where it appears to a superintendent of police that the case is one of great emergency and that in the interest of the state immediate action is necessary, he or she may by a written order give to any constable the authority that could have been given by a justice of the peace by section 9(1). None of these terms are defined.

2.65 In 2014 the Ministry of Justice conducted a review of the powers of entry that exist in various statutory provisions, including the Official Secrets Act 1911. This review was necessitated by section 42(1) of the Protection of Freedoms Act 2012, which states:

> Each Minister of the Crown who is a member of the Cabinet must, within the relevant period—
>
> > (a) review relevant powers of entry, and relevant associated powers, for which the Minister is responsible with a view to deciding whether to make an order under section 39(1), 40 or 41 in relation to any of them,
> >
> > (b) prepare a report of that review, and

(c) lay a copy of the report before Parliament.

2.66 The Ministry of Justice concluded that these powers ought to be retained for the following reason:

> We consider these specific provisions are an essential tool in the protection of national security and the gathering of evidence of offences under this Act is not currently provided for in other more general powers, such as section 8 of PACE. They can only be exercised by police officers following the issue of a warrant.[37]

2.67 We agree that the powers contained in the Police and Criminal Evidence Act 1984 may not necessarily grant the police the powers they need to take sufficiently swift action to safeguard information that relates to national security. For that reason, we agree with the conclusion reached by the Ministry of Justice in 2014.

2.68 Section 6 of the Official Secrets Act 1911 formerly contained a power of arrest. It provided that any person who was found committing an offence contrary to the Official Secrets Act 1911, or was reasonably suspected of having committed, or having attempted to commit, or being about to commit, such an offence, may be apprehended and detained in the same manner as a person who is found guilty of committing a felony.

2.69 This section was repealed in England and Wales, however, by paragraph 1 of Schedule 17(2) to the Serious Organised Crime and Police Act 2005. This repeal took effect from 1 January 2006. This provision was repealed because section 110 of the Serious Organised Crime and Police Act 2005 expanded the power of a constable to arrest a suspect without a warrant contained in section 24 of the Police and Criminal Evidence Act 1984. The provision remains in force in Scotland.

THE POWER TO EXCLUDE THE PUBLIC FROM COURT PROCEEDINGS IN OFFICIAL SECRETS ACT CASES

2.70 Section 8(4) of the Official Secrets Act 1920 gives a court the power to exclude the public from trials for any offences alleged to have been committed under the Official Secrets Acts 1911-1989.[38] A court may exercise this power if, on an

[37] Ministry of Justice, *Powers of Entry Review: Final Report* (November 2014) https://www.gov.uk/government/publications/review-of-powers-of-entry-report (last visited 9 November 2016).

[38] For discussion of some historical cases in which this power was invoked, see R Thomas, *Espionage and Secrecy* (1991) pp 63-85.

application made by the prosecution, the court is satisfied that the publication of any evidence to be given or of any statement to be made in the course of the proceedings would be prejudicial to national security. The passing of sentence must, however, take place in public. Issues surrounding the holding of trials in private will be examined in Chapter 5.

TERRITORIAL AMBIT OF THE OFFENCES

2.71 By virtue of section 10(1) of the Official Secrets Act 1911, the Official Secrets Act 1911 applies to offences committed "in any part of His Majesty's dominions" or by British Officers or subjects elsewhere.

2.72 Section 10(2) provides that:

> An offence under [the Official Secrets Act 1911], if alleged to have been committed out of the United Kingdom, may be inquired of, heard, and determined in any competent British court in the place where the offence was committed, or in England.

2.73 The offences need to have extraterritorial effect given that British assets abroad may be targeted. The offences only apply outside the territorial ambit of the United Kingdom, however, if the defendant is a British Officer or subject. We examine this issue in more detail later on in this chapter.

THE OFFICIAL SECRETS ACT 1920

2.74 The Official Secrets Act 1920 is important in two respects. First, it amends the Official Secrets Act 1911. Secondly, it introduces the presumptions that apply in relation to prosecutions for offences contrary to section 1 of the Official Secrets Act 1911. The Act of 1920 made permanent certain wartime provisions that were deemed necessary to make the Official Secrets Act 1911 more effective.[39] The Official Secrets Act 1920 had two main policy aims:

(1) To put a stop to foreign powers using agents in the United Kingdom for the purposes of espionage.

(2) To remedy the provisions of the Official Secrets Act 1911 which had become ineffective in practice due to more modern methods of spying.

2.75 As already discussed, a number of provisions in the Official Secrets Act 1920 eased the prosecution's burden in respect of proving certain elements of the offences in the Official Secrets Act 1911.

[39] R Thomas, *Espionage and Secrecy* (1991) pp 11-34.

2.76 Thomas is particularly critical of the Official Secrets Act 1920 on the basis that it is incoherent and bears little relation to the legislation it was intended to amend. She states that:

> From a legal perspective, a better solution would have been to repeal the 1911 Act and reorganize the existing and new provisions into a clearer and more logical framework.[40]

2.77 In addition to amending the Official Secrets Act 1911 and introducing the presumptions contained in section 2, the Official Secrets Act 1920 creates a number of free standing offences, which we will now examine.

Section 1 – Unauthorised use of uniforms; falsification of reports, forgery, personation, and false documents

2.78 Section 1(1) of the Official Secrets Act 1920 makes it an offence for any person, with the purpose of gaining admission or assisting any person to gain admission to any prohibited place as defined in the Official Secrets Act 1911, to do any of the following:

(1) use or wear, without lawful authority, any naval, military, air-force, police of other official uniform, or any uniform that resembles the same, as to be calculated to deceive, or holding himself or herself out as a person who is or has been entitled to use or wear any such uniform; or

(2) orally, or in writing in any declaration or application, or in any document signed by him or her or on his or her behalf, knowingly make or connive at the making of any false statement or any omission; or

(3) alter or tamper with any passport or any naval, military, air-force, police, or official pass, permit, certificate, licence, or other document of a similar character (hereinafter in this section referred to as an official document), or have in his or her possession any forged, altered, or irregular official document; or

(4) personate, or falsely represent himself or herself to be a person holding, or in the employment of a person holding office under Her Majesty, or to be or not to be a person to whom an official document or secret official code word or pass word has been duly issued or communicated, or with intent to obtain an official document, secret official code word or pass word, whether for himself or any other person, knowingly make any false statement; or

[40] R Thomas, *Espionage and Secrecy* (1991) pp 12-13.

(5) use, or have in his or her possession or under his or her control, without the authority of the Government department or the authority concerned, any die, seal, or stamp of or belonging to, or used, made or provided by any Government department, or by any diplomatic, naval, military, or air-force authority appointed by or acting under the authority of Her Majesty, or any die, seal or stamp so nearly resembling any such die, seal or stamp as to be calculated to deceive, or counterfeits any such die, seal or stamp, or use, or have in his or her possession, or under his control, any such counterfeited die, seal or stamp;

2.79 Section 1(2) makes it an offence to do any of the following:

(1) retain for any purpose prejudicial to the safety or interests of the state any official document, whether or not completed or issued for use, when he or she has no right to retain it, or when it is contrary to his or her duty to retain it, or fail to comply with any directions issued by any Government department or any person authorised by such department with regard to the return or disposal thereof; or

(2) allow any other person to have possession of any official document issued for his or her use alone, or communicate any secret official code word or pass word so issued, or, without lawful authority or excuse, have in his possession any official document or secret official code word or pass word issued for the use of some person other than himself, or on obtaining possession of any official document by finding or otherwise, neglect or fail to restore it to the person or authority by whom or for whose use it was issued, or to a police constable; or

(3) without lawful authority or excuse, manufacture or sell, or have in his or her possession for sale any such die, seal or stamp as aforesaid.

2.80 By virtue of section 8(2) of the Official Secrets Act 1920, these offences carry a maximum sentence of 2 years' imprisonment if tried in the Crown Court and a maximum sentence of 3 months and/or a fine if tried in a magistrates' court.

2.81 According to section 1(3) of the Official Secrets Act 1920 if the offence requires proof of a purpose prejudicial to the interests of the state, then that term is to be interpreted in the same way as it is interpreted in section 1 of the Official Secrets Act 1911.

2.82 The offences in section 1 are complex. In addition, the language is verbose and the offences contain numerous elements, none of which are defined. For example, there is no definition of "official document".

2.83 Thomas describes these offences as "ancillary espionage crimes". She elaborates in the following terms:

> To gain access to such places [i.e. prohibited places as defined in the Official Secrets Act 1911] during the [First World] War, spies (particularly foreign spies) and their accomplices had engaged in ploys of impersonation and falsifying documents. Thus, the offence of spying was supplemented in 1920 by new crimes [contained in section 1 of the Official Secrets Act 1920].[41]

2.84 Our research has not uncovered any reported prosecutions for these offences.

Section 3 – Interfering with officers or members of Her Majesty's forces

2.85 Section 3 of the Official Secrets Act 1920 makes it an offence for any person in the vicinity of any prohibited place (as defined in the Official Secrets Act 1911) to obstruct, knowingly mislead, or otherwise interfere with or impede, the chief officer or a superintendent or other officer of police, or any member of Her Majesty's forces engaged on guard, sentry, patrol, or other similar duty in relation to the prohibited place.

2.86 In *Adler v George*, the only reported case to consider this provision, the defendant was physically within a prohibited place. The question for the Court of Criminal Appeal was whether this precluded him being guilty of the offence based on the argument that if he was actually in a prohibited place, then it could not be said that he was within the vicinity of it. In rejecting this argument, Lord Parker CJ held that the term "in the vicinity of" ought to be interpreted as "in or in the vicinity of". He elaborated in the following terms:

> Here is a section in an Act of Parliament designed to prevent interference with members of Her Majesty's forces, among others, who are engaged on guard, sentry, patrol or other similar duty in relation to a prohibited place such as this station. It would be extraordinary, I venture to think it would be absurd, if an indictable offence was thereby created when the obstruction took place outside the precincts of the station, albeit in the vicinity, and no offence at all was created if the obstruction occurred on the station itself.[42]

2.87 As with the offences in section 1, there is little evidence of these offences being used in practice in the modern era.

[41] R Thomas, *Espionage and Secrecy* (1991) p 14.

[42] *Adler v George* [1964] 2 QB 7; [1964] 2 WLR 542, 10.

2.88 By virtue of section 8(2) of the Official Secrets Act 1920, these offences carry a maximum sentence of 2 years' imprisonment if tried in the Crown Court and a maximum sentence of 3 months and/or a fine if tried in a magistrates' court.

Section 6 – Duty of giving information as to the commission of offences

2.89 By virtue of section 6(1), the powers in section 6 of the Official Secrets Act 1920 can only be exercised if a chief officer of police (or someone nominated by him or her under section 6(3)) has reasonable grounds for suspecting that an offence contrary to section 1 of the Official Secrets Act 1911 has been committed and he or she believes that information relating to the offence or suspected offence can be provided by a specific individual. If both these criteria are satisfied, then the chief officer of police can apply to the Secretary of State for permission to exercise the powers conferred by section 6.

2.90 If the Secretary of State gives his or her permission, then a police officer not below the rank of inspector can require the individual in question to give any information relating to the offence or suspected offence and, if so required, to attend a place specified by the police officer.

2.91 An individual who fails to comply with the request for information, or fails to attend the specified place, commits a criminal offence.

2.92 By virtue of section 6(2), if the chief officer of police has reasonable grounds to believe that the case is one of great emergency, then he or she does not need to seek the authorisation of the Secretary of State. He or she must, however, report the circumstances to the Secretary of State "forthwith". There is no definition of this term.

2.93 By virtue of section 8(2) of the Official Secrets Act 1920, these offences carry a maximum sentence of 2 years' imprisonment if tried in the Crown Court and a maximum sentence of 3 months and/or a fine if tried in a magistrates' court.

2.94 As originally drafted, this provision applied to any offence in the Official Secrets Act 1911. It was narrowed by the Official Secrets Act 1939, however, so that it only applied to the offence in section 1 of the Official Secrets Act 1911.

2.95 Thomas gives some examples of this offence being used. In 1937 a journalist named Ernest Lewis was convicted under section 6 for failing to name the source who had passed him official information. In 1939 Duncan Sandys MP was questioned by the Attorney General about his sources of information concerning the inadequacies of the air defences around London.[43] According to Williams,

[43] R Thomas, *Espionage and Secrecy* (1991) p 18.

Sandys was also threatened with prosecution under this section and possibly only Parliamentary privilege prevented it.[44]

Section 7 – Attempts and incitement

2.96 Section 7 of the Official Secrets Act 1920 contains a number of provisions that criminalise acts that are preparatory to the commission of an offence under the Official Secrets Acts.

2.97 There is a specific provision in section 7 of the Official Secrets Act 1920 that criminalises any person who attempts to commit an offence contained within that legislation or the Official Secrets Act 1911. This section was not repealed when the Criminal Attempts Act 1981 created a general statutory offence of attempt. The conduct element of an attempt under the 1981 Act is an act that is *more than merely preparatory* to the commission of the substantive offence.[45] Section 7 of the Official Secrets Act 1920 also makes it an offence to do an act that is *preparatory* to the commission of an offence. Section 7 therefore encompasses conduct that would not fall within the scope of a criminal attempt under the 1981 Act.

2.98 Section 7 of the Official Secrets Act 1920 also makes it an offence for any person to solicit, incite or endeavour to persuade another person to commit an offence within that legislation or the Official Secrets Act 1911. Offences such as these were not uncommon prior to the enactment of the offences found in Part 2 of the Serious Crime Act 2007. Part 2 of the Serious Crime Act 2007 abolished the common law offence of incitement and replaced it with offences that criminalise an individual who does acts capable of assisting or encouraging another to commit an offence. Despite the creation of these general offences of assisting or encouraging, section 7 of the Official Secrets Act 1920 was not repealed by the Serious Crime Act 2007 and remains in force.

2.99 The Court of Appeal considered the meaning of the term "act preparatory to the commission of an offence" in *Bingham.*[46] In this case Lord Widgery CJ stated that an individual will commit an offence under section 7 of the Official Secrets Act 1920 if he or she does an act that "opens the door to the commission of an offence".[47] Lord Widgery CJ also confirmed that if all the elements of the

[44] D Williams, *Not in the Public Interest* (1965) pp 71-75.

[45] D Ormerod and K Laird, *Smith and Hogan's Criminal Law* (14th edn, 2015), p 470 and A P Simester, J R Spencer, F Stark, G R Sullivan and G J Virgo, *Simester and Sullivan's Criminal Law* (6th edn, 2016), p 340.

[46] *R v Bingham* [1973] QB 870; [1973] 2 WLR 520. See also, *R v Oakes* [1959] 2 QB 350; [1959] 2 WLR 694.

[47] *R v Bingham* [1973] QB 870; [1973] 2 WLR 520, 875.

substantive offence are not present, for example because the individual in question was not doing an act that would be prejudicial to the interests of the state, then he or she cannot be guilty of doing an act preparatory to the commission of an offence in section 7 of the Official Secrets Act 1920.

2.100 The Court of Appeal also confirmed that the prosecution need only show that commission of the substantive offence was possible. Lord Widgery CJ upheld the following direction that was given by the trial judge:

> The prosecution only had to show that at the time of doing the act the accused realised that the transmission of prejudicial information was possible.[48]

2.101 The Court of Appeal therefore refused to narrow the phrase "act preparatory to the commission of an offence", which would have made the passing of information insufficient to support the charge.

2.102 Finally, section 7 of the Official Secrets Act 1920 also makes it an offence to aid or abet the commission of an offence under the Official Secrets Acts. This supplements the general provisions of aiding, abetting, counselling or procuring an offence that are contained in the Accessories and Abettors Act 1861. Although there is no case law considering this provision, presumably it would be interpreted in the same way as the offences in the Accessories and Abettors Act 1861, with a similar fault element.[49]

THE OFFICIAL SECRETS ACT 1939

2.103 The sole effect of the Official Secrets Act 1939 is to substitute a new section 6 in the Official Secrets Act 1920. As we have already explained, section 6 of the Official Secrets Act 1920 creates a duty of giving information as to the commission of offences under the Official Secrets Acts. The Official Secrets Act 1939 amended section 6 of the Official Secrets Act 1920 so that the duty only applies in respect of offences contrary to section 1 of the Official Secrets Act 1911.

PROBLEMS WITH THE CURRENT LAW

2.104 In this section, we will examine the extent to which there are any problems with the current law and ask consultees' views on how they could be remedied. At the outset, it is important to reiterate that the Official Secret Act 1911 re-enacted the

[48] *R v Bingham* [1973] QB 870; [1973] 2 WLR 520, 876.

[49] D Ormerod and K Laird, *Smith and Hogan's Criminal Law* (14th ed 2015) pp 224-237. A P Simester, J R Spencer, F Stark, G R Sullivan and G J Virgo, *Simester and Sullivan's Criminal Law* (6th ed 2016) pp 228-229.

Official Secrets Act 1889 with amendments. Many of its provisions, therefore, have their origin in the nineteenth century. The consequence of this is that the Official Secrets Act 1911 does not reflect how statutes are drafted in the modern era. The same is true, albeit to a lesser extent, of the Official Secrets Acts 1920 and 1939. This presents not only a problem of presentation, as the legislation is more complex than it would otherwise need to be, but also a problem of substance, as it is sometimes unclear what the provisions are intended to protect against. These issues are also evident from the fact the legislation uses archaic language, such as "die, seal or stamp" and does not reflect how information is stored in the digital era. For example, some might question whether the term "official document" would encompass information stored digitally. There is a need to adopt language that will ensure the offences are future proofed against developing technology and techniques in espionage.

2.105 Aside from these general problems, initial consultation with stakeholders suggests the existence of a number of other problems with the Official Secrets Act 1911-1939. This section will examine these problems and suggest some ways they could be remedied.

There must be an enemy

2.106 The offences in section 1 of the Official Secrets Act 1911 criminalise the following conduct:

(1) making any sketch, plan, model, or note which is calculated to be or might be or is intended to be directly or indirectly useful to an enemy; or

(2) obtaining, collecting, recording, publishing, or communicating to any other person any secret official code word, or pass word, or any sketch, plan, model, article, or note, or other document or information which is calculated to be or might be or is intended to be directly or indirectly useful to an enemy.

2.107 An offence is only committed if the defendant, at the time he or she engaged in this conduct, did so with a purpose that is prejudicial to the safety or interests of the state. We discussed the meaning of this key phrase earlier in this chapter.

2.108 As we have already discussed, at the time the legislation was being debated in the House of Lords the suggestion was made to replace the term "enemy" with the term "foreign power". This amendment was rejected and a search of Hansard has not revealed why this was the case. The Official Secrets Act 1920 does, however, use the terms "foreign power" and "foreign agent" instead of "enemy".

2.109 In one of the early prosecutions for an offence contrary to the Official Secrets Act 1911 it was held that the term "enemy" should be construed so as to include any potential enemy. Despite this clarification, our initial consultation with stakeholders suggests that this term causes problems in practice. The same view was expressed a number of years ago by the Intelligence and Security Committee of Parliament. In 2004 the Committee observed that:

> A further problem is raised by the expression in the 1911 Act, "useful to an enemy", which raises not only problems of construction, but the

danger of giving unnecessary offence to states with which the UK is not at war.[50]

2.110 To elaborate further, first, even if it could be proven that an individual communicated information that would be directly useful to a hostile state, having to designate that state in court as an enemy of the United Kingdom could have negative diplomatic consequences. Related to this is the fact an individual may communicate sensitive information to another state intending that it will be used to injure the United Kingdom, where the state in question could never properly be described as an enemy or even a potential enemy.

2.111 For example, Daniel Houghton offered to sell the names of agents working for the Secret Intelligence Service, in addition to details about information gathering software, to the Dutch Intelligence Agency. Mr Houghton pleaded guilty to an offence contrary to section 1(1) of the Official Secrets Act 1989, so the question of whether the Netherlands could be regarded as an enemy or potential enemy never arose.[51] Assuming that this matter is a question of fact for the jury, it is unlikely, however, a jury would conclude that the Netherlands falls into either of these two categories.

2.112 The legislation was drafted with a very specific enemy in mind, namely Germany under the rule of the Kaiser. This does not reflect the reality of the situation currently faced by the United Kingdom, whereby an individual may be acting for the benefit of a terrorist organisation rather than a state. Although the term "enemy" seems sufficiently broad to encompass an organisation as opposed to a state, the legislation was drafted with reference to states. It is therefore unclear whether a court would construe it broadly to encompass non-state organisations.

Provisional conclusion 1

2.113 **We provisionally conclude that the inclusion of the term "enemy" has the potential to inhibit the ability to prosecute those who commit espionage. Do consultees agree?**

2.114 The difficulty in addressing this problem is the fact that the offences contained in section 1 of the Official Secrets Act 1911 have the potential to be broad offences that criminalise conduct that is not intended to prejudice the state. One of the ways the offences are made narrower is the fact that the information that was

[50] Intelligence and Security Committee: Annual Report 2003-2004 (2004) Cm 6240 p 43. The Committee as currently constituted has not expressed any view on the Official Secrets Acts 1911-1989.

[51] "Former MI6 man sentenced for secret files leak" (*BBC News,*3 September 2010*)* http://www.bbc.co.uk/news/uk-england-london-11176434 (last visited 9 November 2016).

communicated, or the sketch that was made, must be calculated to be, or might be, or is intended to be directly or indirectly useful to an enemy. Whilst replacing the term "enemy" with one that is more neutral might have the effect of addressing the problem that stakeholders have brought to our attention, it could potentially widen the scope of the offence.

2.115 We provisionally agree with the conclusion reached by the Intelligence and Security Committee of Parliament, that the term "enemy" is problematic and ought to be replaced. We note, however, the risk that substituting for the term "enemy" another term without making any further changes to the legislative language risks upsetting the balance of the offence. In particular, we have been mindful of the following considerations:

(1) The need to ensure that any amendment does not render the offences in section 1 of the Official Secrets Act 1911 overly broad. In this respect, it is important to bear in mind that a prosecution for an offence contrary to the Official Secrets Act 1911 can only be initiated with the consent of the Attorney General. We discuss the role of the Attorney General in more detail in Chapter 3.

(2) The need to ensure that the espionage offence encompasses not only states, but also non-state entities such as terrorist organisations in addition to entities that are directed and controlled by a foreign government or governments.

2.116 As our comparative law research has demonstrated, examples of espionage offences from other jurisdictions suggest there are viable modern alternatives to using the term "enemy". These alternative terms, however, cannot necessarily be incorporated into any amended version of the Official Secrets Act 1911. This is because in these other jurisdictions, these terms are used to describe the person to whom the information is communicated, rather than the character the information must have before its communication will constitute a criminal offence. It is the fact that the information that was communicated must be calculated to be, or might be, or is intended to be directly or indirectly useful to an enemy that helps to ensure the offence is not overly broad.

Options for reform

THE NATURE OF THE OFFENCE

2.117 Before proceeding to describe how the offence in the 1911 Act could be reformulated to remove the problems attributable to the use of the term "enemy", we believe it is first necessary to examine in greater detail the type of conduct the provisions are intended to criminalise.

2.118 As we stated above, the Security Service describes espionage in the following terms:

> Espionage is the process of obtaining information that is not normally publicly available, using human sources (agents) or technical means (like hacking into computer systems). It may also involve seeking to influence decision-makers and opinion-formers to benefit the interests of a foreign power.[52]

2.119 There are two aspects of the offences contained in section 1 of the Official Secrets Act 1911 that we believe are the essence of the criminal offence of espionage. First, the fact that the defendant acted in a way that was prejudicial to the safety or interests of the United Kingdom (as to whether these should be limited to national security matters, see below). Secondly, the fact that the conduct that has some connection with a foreign power. We believe these features ought to be explicitly included in some form in any remodelled offence.

2.120 Before proceeding to describe how the offence could be reformed so that these elements are explicitly included, it is worth examining more closely the elements of the offence so that we can consider how best to address the problem that has been brought to our attention without generating further difficulties in application.

2.121 The current offences under s 1(1)(b) and (c) under the 1911 Act consist of the following elements:

(1) A defendant – note that there is no requirement that the person be a Crown servant, government contractor or notified person. Therefore, like the vast majority of criminal offences, the offence can be committed by anyone in the United Kingdom and by a British officer or subject outside the United Kingdom.

(2) Proscribed conduct - making any sketch, plan, model, or note; collecting, recording, publishing, or communicating the material in question.

(3) The defendant must (subjectively) hold a purpose to achieve a particular objective by his conduct.

(4) The purpose held by the defendant must, objectively viewed, be prejudicial to the state's safety or its interests. We discussed the meaning of these terms earlier in this chapter.

(5) A relationship to an enemy or potential enemy:

[52] https://www.mi5.gov.uk/espionage (last visited 9 November 2016).

(a) the relevant information (collected etc.) must be calculated to be or might be or is directly or indirectly useful to an enemy, including a potential enemy. This entails an objective assessment of whether the material is likely to be of such use, not a subjective determination as to whether the defendant thinks it is likely to be of such use; or

(b) the information was intended by the defendant to be of use to an enemy, or potential enemy.

(6) There is no restriction on the characteristics of the person to whom the material is disclosed.

ELEMENTS OF THE OFFENCE TO BE RETAINED

2.122 We believe that several elements of the offence must be retained in substance even if redrafted in more modern form.

(1) There should continue to be no restriction on the categories of person who can commit the offence. We believe that artificially narrowing the pool of persons to whom the offence applies could cause problems in practice, as potentially anyone could be induced to obtain information that is not publicly available. In addition, given that the overwhelming majority of criminal offences can be committed by anyone within the United Kingdom, there needs to be some specific justification for limiting the applicability of an offence and we can find none here. It will be recalled that the offence can also be committed by a British officer or subject not inside the United Kingdom.

(2) The offence should continue to be capable of being committed by someone who not only communicates information, but also by someone who obtains or gathers information.

(3) The offence currently applies to any secret official code word, or pass word, or any sketch, plan, model, article, note, or other document or information. We believe, however, that most of these terms are superfluous and that "information" would suffice.

Provisional conclusion 2

2.123 **Any redrafted offence ought to have the following features:**

(1) Like the overwhelming majority of criminal offences, there should continue to be no restriction on who can commit the offence;

(2) The offence should be capable of being committed by someone who not only communicates information, but also by someone who obtains or gathers it. It should also continue to apply to those who approach, inspect, pass over or enter any prohibited place within the meaning of the Act.

(3) The offence should use the generic term "information" instead of the more specific terms currently relied upon in the Act.

Do consultees agree?

ADDITIONAL ELEMENTS OF A REFORMULATED OFFENCE

2.124 As we have already discussed, the connection of the prohibited activity to the interests of a foreign power and the aim to prejudice the United Kingdom's safety or interests are the essence of espionage. We believe both of these ought to feature in some form in any reformulated offence. The following section will examine how they could be included.

2.125 To reformulate the offence, we need to examine:

(1) The element of "the safety or interests of the state".

(2) Whether it is necessary for the element of prejudice to the United Kingdom's safety or interests to involve proof of subjective fault.

(3) The relationship that must exist between the conduct of the defendant and a foreign power.

(4) What foreign power might mean in this context.

(5) Whether the element relating to foreign power requires proof of fault.

"Safety or interests of the state"

2.126 As we discussed previously, in *Chandler and others v Director of Public Prosecutions*, the phrase "interests of the state", was interpreted to mean the objects of state policy determined by the Crown on the advice of Ministers.

2.127 It could be argued that the phrase "safety or interests of the state" gives the offence too broad a scope if the 1911 Act requirement for the information to be "useful to an enemy", with its obvious overtones of security and defence issues, is replaced by a broader concept extending to any "foreign power" (as discussed below). Arguably, agents of foreign powers routinely gather considerable amounts of information for the benefit of a foreign power with the intention of prejudicing the political interests of the United Kingdom, but few people would consider that all such conduct should amount to the criminal offence of espionage.

2.128 One way of providing a greater degree of specificity is to use the term "national security" rather than "safety or interests". Although consultees may take the view that this term suffers from the same lack of precise definition as the term "safety or interests", the Grand Chamber of the European Court of Human Rights in

Kennedy v United Kingdom accepted that, "By the nature of things, threats to national security may vary in character and may be unanticipated or difficult to define in advance."[53] The Grand Chamber accepted that the meaning of this term was sufficiently clear to satisfy the requirement in Article 8(2) of the European Convention on Human Rights that legislation infringing the right to respect for private and family life must be sufficiently precise in order to satisfy the Convention.

Consultation question 1

2.129 **Should the term "safety or interests of the state", first used in the 1911 Act, remain in any new statute or be replaced with the term "national security"?**

Conduct prejudicial to the safety or interests of the state/national security

2.130 As we have already discussed, a key feature of section 1 of the Official Secrets Act 1911 is the fact the defendant acted with a purpose "prejudicial" to the safety or interests of the state. We analysed earlier how this element of the offence has been interpreted. In short, the defendant must have a specific purpose in mind (for example disrupting an airbase), which must objectively prejudice the safety or interests of the United Kingdom. The defendant's opinion as to whether his conduct prejudices the safety or interests of the United Kingdom is irrelevant.

2.131 To ensure the elements of any reformulated offence are as clear as possible and to maximise consultees' opportunity to comment upon them, we believe it is necessary to set out in detail the relevant elements.

2.132 The elements are illustrated by the facts of *Chandler*:

(1) the defendant intentionally trespassed on the airbase, which was a prohibited place within the meaning of section 3 of the Official Secrets Act 1911;

(2) the defendant subjectively had as his purpose the disruption of the airbase;

(3) objectively there was prejudice to the safety or interests of the United Kingdom from his intentional disruption of the airbase.

2.133 At present what is arguably the most important element of the offence – prejudice to the safety or interests of the state – has no fault element at all. Given the

[53] *Kennedy v United Kingdom* (2011) 52 EHRR 4, [159].

seriousness of the offence, we believe it is important for this element of the offence to incorporate a subjective fault element.

2.134 For that reason, we have taken the view that an offence should only be committed if the defendant, in intentionally engaging in the proscribed conduct, knew, or had reasonable grounds to believe that his or her conduct may cause prejudice to the safety or interests of the state.

2.135 At this stage it is important to point out that the offence would not require the prosecution to demonstrate actual prejudice to the safety or interests of the state. The offence would therefore be similar to the offence contained in section 1(2) of the Criminal Damage Act 1971. By virtue of this provision a person commits an offence if he or she destroys or damages any property, intending to destroy or damage any property or being reckless as to whether any property would be destroyed or damaged. The person only commits an offence if he or she intends by the destruction or damage to endanger the life of another or is reckless as to whether the life of another would be thereby endangered.

2.136 In *Parker* the defendant was convicted of the offence in section 1(2) of the Criminal Damage Act 1971 when he started a fire in his semi-detached house.[54] The Court of Appeal upheld his conviction on the basis that the fact that his neighbours were absent and therefore never at risk did not preclude a conviction. The same approach would apply to our remodelled offence.

Consultation question 2

2.137 **Do consultees have a view on whether an individual should only commit an offence if he or she knew or had reasonable grounds to believe that his or her conduct might prejudice the safety or interests of the state / national security?**

The connection between the conduct and a foreign power

2.138 This element of the offence seeks to ensure that the offence is limited to cases where there is not only knowledge or reasonable grounds to believe that the conduct might harm the interests of the United Kingdom as we have just discussed, but that the conduct might benefit a foreign power. The foreign element inherent in espionage is currently reflected in the current law through the use of the term “enemy”. The term enemy is problematic, however, for the reasons we explained earlier. It is therefore necessary for us to consider suitable alternatives.

[54] *Parker* [1993] *Criminal Law Review* 856.

What is a foreign power?

2.139 As noted at the outset, the entities potentially engaged in attempts to access sensitive information vary considerably. By way of example, Allen Ho, a naturalised citizen of the United States, has recently been indicted in the United States for running an espionage ring aimed at obtaining information relating to the nuclear industry.[55] According to the Department of Justice, "The arrest and indictment in this case sends an important message to the United States nuclear community that foreign entities want the information you possess."

2.140 The increasing power of companies within state structures, and complex governance models, can make it difficult to determine whether an entity such as a company is acting in a private capacity or as an emanation of the state. Further, in some instances it is clear that companies may be under state control, or have a majority stake owned by governments, where the nature of the investments is non-commercial, but rather an instrument of policy making. It is desirable that any new offence should be flexible in accommodating the different ways in which foreign power may be exercised. A failure to do so would render the offence ineffective.

2.141 The range of entities that need to be included is potentially quite broad. By way of example, the Espionage Statutes Modernization Bill was introduced into the Congress of the United States in 2011 with the aim of, "improving, modernising, and clarifying the espionage statutes" in force in the United States. The bill would have replaced the term "foreign nation" in the Espionage Act 1917 with the term "foreign power", which would have encompassed the following entities:

(1) A foreign government or any component thereof, whether or not recognised by the United States.[56]

(2) A faction of a foreign nation or nations, not substantially composed of United States persons.[57]

(3) An entity that is openly acknowledged by a foreign government or government to be directed and controlled by such foreign government or governments.[58]

[55] https://www.justice.gov/opa/pr/us-nuclear-engineer-china-general-nuclear-power-company-and-energy-technology-international (last visited 22 November).

[56] This would ensure that the offence criminalises those who communicate information to another state, even if it is a state with which the United Kingdom is not at war

[57] This would encompass those factions that cannot be characterised as states, but which may nevertheless seek to gain access to sensitive information by convert means.

(4) A group engaged in international terrorism or activities in preparation therefor.[59]

(5) A foreign based political organisation, not substantially composed of United States persons.[60]

(6) An entity that is directed and controlled by a foreign government or governments.[61]

(7) An entity not substantially composed of United States persons that is engaged in the international proliferation of weapons of mass destruction.[62]

2.142 We are using this list to demonstrate the approach that was considered appropriate by some in the United States and invite consultees' views on whether the list of foreign entities contained in the Espionage Statutes Modernization Bill is suitable for use in the domestic context to replace the unsatisfactory element of enemy.

2.143 We are not, however, suggesting that this list ought to be incorporated wholesale into domestic law. One issue that would need to be overcome is that any list would need to be adapted for use in the domestic context. For example, should it refer only to British citizens or – as seems more appropriate - also residents of the United Kingdom who are non-citizens?

Consultation question 3

[58] This would encompass those entities that, whilst not governments in themselves, are openly acknowledged as being directly controlled by a foreign governments and could be used to obtain access to sensitive information.

[59] As we discussed earlier, one of the problems with the current law is that it is unclear whether it encompasses non-state entities. This category would remedy that problem.

[60] Including this category would ensure that the offence would be committed if the information were communicated not to the government of a nation, but, for example, to an opposition party seeking to overthrow the government.

[61] The rationale for including this category has been explained above. The difference here, however, is that the entity may not be acknowledged as being directed and controlled by a foreign government.

[62] This once again ensures that those entitles engaged in terrorism are encompassed by the offence.

2.144 **Is the list of foreign entities contained in the Espionage Statutes Modernization Bill a helpful starting point in the domestic context? Do consultees have views on how it could be amended?**

Incorporating the element relating to the foreign power

2.145 One very narrow approach would be to require proof that the defendant was acting as an agent of a foreign power in the strict sense of that term. That, however, would be too narrow.

2.146 Alternatively, the relationship or connection might best be described as one where the defendant engages in the relevant conduct with an awareness or some commitment to the idea that he or she is engaging in that conduct with a view to furthering the interests or potential interests of a foreign power.

2.147 A requirement for the prosecution to prove that the defendant's conduct did in fact benefit a foreign power could be very difficult given the nature of the activity in question.

2.148 We therefore consider that a better approach would be to focus on whether the defendant knew or believed that his conduct might benefit a foreign power.

2.149 We are not drafting a statute at this stage so what is important is that we can be confident that the requisite connection between the individual and the foreign power can be translated into statutory language. We are confident that it can, and derive confidence from the fact that other statutory offences include elements that the defendant's conduct must be performed for the benefit of another. We have found the offence of handling stolen goods, which is contained in section 22 of the Theft Act 1968 useful in this regard.

Provisional conclusion 3

2.150 **We have provisionally concluded that an offence should only be committed if the defendant knew or had reasonable grounds to believe his or her conduct was capable of benefiting a foreign power. Do consultees agree?**

CONCLUSION

2.151 As a result of the discussion in this section, a person would commit an offence if he or she:

(1) makes any sketch, plan, model, or note; collects, records, publishes, or communicates any information;

(2) knows or has reasonable grounds to believe that his or her conduct might prejudice the safety or interests of the state / national security;

(3) knows or has reasonable grounds to believe that his or her conduct is capable of benefiting a foreign power;

(4) intends thereby to prejudice the [national security/safety or interests] of the United Kingdom or is reckless as to whether the [national security/safety or interests] of the United Kingdom would be prejudiced.

2.152 As we have explained, we would welcome consultees' views on the suitability of a number of these elements.

2.153 Before concluding, it is important to point out that any reformulated offence would be capable of being committed in inchoate form: attempts, conspiracy and assisting and encouraging espionage would all be criminal.

2.154 For example, if a person assisted or encouraged another to engage in the conduct we analysed above, then he or she would be guilty of assisting or encouraging espionage by virtue of the offences contained in Part 2 of the Serious Crime Act 2007.[63] If an individual attempted to engage in any of these forms of conduct, then he or she would be guilty of any attempt by virtue of the Criminal Attempts Act 1981 or by virtue of section 7 of the Official Secrets Act 1911, which we discussed above.[64] Finally, if two or more people agreed to pursue a course of conduct that would necessarily amount to the commission of espionage, then they would be guilty of conspiracy by virtue of the Criminal Law Act 1977.[65] These latter two provisions ensure that conduct is criminalised at a sufficiently early stage to minimise the risk of the proscribed consequences from actually eventuating.

The focus on military installations

2.155 As our discussion of the current law demonstrates, the Official Secrets Act 1911 contains an extensive list of "prohibited places".[66] Our initial consultation with stakeholders, however, suggests that this list is under-inclusive. This is because the primary focus of the list is upon sites that are military in nature. In the modern era sensitive information that needs protection from being targeted is not only held on sites which are military in nature, but upon sites which may have a variety of uses. Linked to this issue is the fact the legislation does not protect sites that store sensitive economic information that may also be targeted by those with intent to injure the national interest. Finally, given when it was enacted, the

[63] D Ormerod and K Laird, *Smith and Hogan's Criminal Law* (14th edn, 2015), p 470 and A P Simester, J R Spencer, F Stark, G R Sullivan and G J Virgo, *Simester and Sullivan's Criminal Law* (6th edn, 2016), p 340.

[64] D Ormerod and K Laird, *Smith and Hogan's Criminal Law* (14th edn, 2015), p 459 and A P Simester, J R Spencer, F Stark, G R Sullivan and G J Virgo, *Simester and Sullivan's Criminal Law* (6th edn, 2016), p 343.

[65] D Ormerod and K Laird, *Smith and Hogan's Criminal Law* (14th edn, 2015), p 484 and A P Simester, J R Spencer, F Stark, G R Sullivan and G J Virgo, *Simester and Sullivan's Criminal Law* (6th edn, 2016), p 313.

[66] As we discussed earlier, although the list may be amended, this power has been exercised infrequently over the years.

Official Secrets Act 1911 makes no reference to the critical national infrastructure. This is defined as:

> Those critical elements of infrastructure (namely assets, facilities, systems, networks or processes and the essential workers that operate and facilitate them), the loss or compromise of which could result in:
>
> > a) major detrimental impact on the availability, integrity or delivery of essential services – including those services, whose integrity, if compromised, could result in significant loss of life or casualties – taking into account significant economic or social impacts; and/or
> >
> > b) significant impact on national security, national defence, or the functioning of the state.[67]

2.156 Arguably, this is problematic given that, according to the Centre for the Protection of National Infrastructure, these assets are also under threat from espionage related activity.[68]

2.157 These provisions in the Official Secrets Act 1911 stand in stark contrast to sections 128 – 131 of the Serious Organised Crime and Police Act 2005. These provisions relate to "protected sites". Section 128(1A) of the Serious Organised Crime and Police Act 2005 defines a "protected site" as either a "nuclear site" or a "designated site". The Secretary of State may designate a site only if the following conditions are satisfied:

(1) the site is comprised in Crown land; or

(2) the site is comprised in land belonging to Her Majesty in Her private capacity or to the immediate heir to the Throne in his private capacity; or

(3) it appears to the Secretary of State that it is appropriate to designate the site in the interests of national security.

2.158 Despite the fact that the provisions have similar purposes, there is an inconsistency between the list of prohibited places in the Official Secrets Act 1911 and the list of protected sites in the Serious Organised Crime and Police Act 2005. This is problematic for two reasons. Some sites may be categorised as being "designated sites" but are not "prohibited places" for the purposes of the

[67] http://www.cpni.gov.uk/about/cni/ (last visited 9 November 2016)

[68] http://www.cpni.gov.uk/threats/espionage/ (last visited 9 November 2016)

Official Secrets Act 1911, meaning that they are not necessarily being adequately protected. Conversely, a site may be a "prohibited place" but not "a designated site", giving rise to the same problem.

2.159 Given the enactment of sections 128 – 131 of the Serious Organised Crime and Police Act 2005, it could be argued that there is no longer a need to have a parallel list of prohibited places. The 2005 Act provisions can be summarised as follows:

(1) Section 128 – makes it an offence for a person to trespass upon any protected site.

(2) Section 129 – creates a corresponding offence to the one in section 128 that applies in Scotland.

(3) Section 130 – makes the offences in sections 128 and 129 arrestable offences.

(4) Section 131 – provides that if a site is designated by the Secretary of State, then various statutory provisions that grant public rights of access do not apply. It also imposes an obligation on the Secretary of State to take such steps as he or she considers appropriate to inform the public of the effect of any designation order, including, in particular, displaying notices on or near the site to which the order relates.

2.160 In the modern era, sites that store sensitive information require just as much protection as sites that store "munitions of war". This is reflected in section 128 of the Serious Organised Crime and Police Act 2005 and the fact a site may be designated despite the fact it is not a military installation. That section 3 of the Official Secrets Act 1911 is predominately concerned with the latter reflects the fact it was drafted in the years immediately preceding the First World War.

Provisional conclusion 4

2.161 **The list of prohibited places no longer accurately reflects the types of site that are in need of protection. Do consultees agree?**

2.162 One way to remedy this problem is to rely upon the *approach* taken in the Serious Organised Crime and Police Act 2005 namely one of designating sites. It would be possible to create a new statutory power to designate sites if it were in the interests of national security to do so. This would ensure the legislation is capable of meeting contemporary challenges. Such a list would be enacted in primary legislation, but would be capable of amendment by way of the affirmative resolution procedure. We do not, however, believe that this power should only apply to Crown / Royal land.

Consultation question 4

2.163 **We consider that a modified version of the approach taken in the Serious Organised Crime and Police Act 2005 is a suitable alternative to the current regime. The Secretary of State would be able to designate a site as a "protected site" if it were in the interests of national security to do so. Do consultees agree?**

Archaic provisions

2.164 As was typical of the Edwardian era, the legislation is drafted in a verbose fashion and contains a number of provisions that may have been necessary in 1911, but seem somewhat quaint today. For example the section 1 of the Official Secrets Act 1920 makes it an offence for a person to do the following with intention to gain access to a prohibited place:

> Use, or have in his or her possession or under his or her control, without the authority of the Government department or the authority concerned, any die, seal, or stamp of or belonging to, or used, made or provided by any Government department, or by any diplomatic, naval, military, or air-force authority appointed by or acting under the authority of His Majesty, or any die, seal or stamp so nearly resembling any such die, seal or stamp as to be calculated to deceive, or counterfeits any such die, seal or stamp, or uses, or has in his or her possession, or under his control, any such counterfeited die, seal or stamp;

We are unaware of examples of this offence ever being prosecuted. The continued existence of provisions such as this one, which makes reference to die and stamps, makes the legislation archaic and unreflective of the modern world.

Provisional conclusion 5

2.165 **There are provisions contained in the Official Secrets Acts 1911-1939 that are archaic and in need of reform. Do consultees agree?**

2.166 Related to this problem is the overarching issue that the Official Secrets Acts 1911-1939 were enacted long before the digital age. The references made in the legislation to sketches, plans, models, notes and secret official pass words and code words are anachronistic. These terms could be replaced by a sufficiently broad generic term. The aim is to future proof the legislation against developments in technology and espionage techniques.

2.167 We believe there are a number of more generic terms that could be used that would ensure the legislation accurately reflects the type of information in need of protection. For example, section 8 of the Fraud Act 2006 defines the term "article" as "any program or data held in electronic form."[69] A term such as this one is sufficiently generic not only to ensure the legislation achieves its stated aim, but also ensures that it would not become quickly out of date. Whilst we do not

[69] See D Ormerod and K Laird, *Smith and Hogan's Criminal Law* (14th edn, 2015), pp 1037-1038. A P Simester, J R Spencer, F Stark, G R Sullivan and G J Virgo, *Simester and Sullivan's Criminal Law* (6th edn, 2016), pp 622-625.

disagree with the proposition that seals and "secret official code words" are in need of protection, we believe there are more modern, generic terms that could be used that would not give rise to the possibility of creating gaps in the legislation.

Provisional conclusion 6

2.168 **We consider that the references in the Official Secrets Acts 1911 and 1920 to sketches, plans, models, notes and secret official pass words and code words are anachronistic and in need of replacement with a sufficiently general term. Do consultees agree?**

The territorial ambit of the offences

2.169 The criminal law is territorial, which means that "misconduct committed outside the realm cannot ordinarily amount to the conduct element of an offence under English law".[70] The courts in England and Wales have typically adopted a terminatory approach to jurisdiction. This means that the courts will accept jurisdiction to try an offence when the "last act" was performed in this jurisdiction or, if the offence is a result crime, when the prohibited result occurred in this jurisdiction. In some cases, however, the courts have taken a more flexible approach. In *Smith (No 4),* the Court of Appeal preferred, on policy grounds, to apply a more flexible test, giving the English courts a broader jurisdiction over conduct where "a substantial measure of the activities constituting the crime take place in England".[71] The validity of this approach was confirmed by the Court of Appeal more recently in *Rogers* and *Sheppard*.[72]

2.170 The Official Secrets Act 1911 provides that an offence can be committed by someone outside the United Kingdom if he or she is a British Officer of subject, which means that it has extraterritorial effect.

2.171 It is necessary to consider, however, whether the territorial ambit of the offences is sufficient to provide adequate protection to assets abroad. For example, an individual who is not a British Officer or subject could engage in the conduct prohibited by the Official Secrets Act 1911 in a British embassy abroad. Due to the fact that this individual is not a British Officer or subject, he or she commits no offence.

[70] M Hirst, *Jurisdiction and the Ambit of the Criminal Law* (2003), p 3. See also G Williams, "Venue and the Ambit of the Criminal Law (Part 3)" (1965) 81 *Law Quarterly Review* 518.

[71] *R v Smith (No 4)* [2004] EWCA Crim 631; [2004] 3 WLR 229 at [55].

[72] *R v Rogers* [2014] EWCA Crim 1680; [2015] 1 WLR 1017 at [54]; *R v Sheppard* [2010] EWCA Crim 65; [2010] 1 WLR 2779.

2.172 There have been recent legislative changes that have recognised the necessity of expanding the territorial ambit of certain offences. The recent changes made to the Computer Misuse Act 1990 by the Serious Crime Act 2015 are a good example of this.

2.173 Under that legislation as amended, an individual can commit an offence contrary to the Computer Misuse Act 1990 even if they were outside the United Kingdom when they are alleged to have committed the offence provided there is a "significant link" with the United Kingdom. The Act defines "significant link" in a number of different ways.[73]

2.174 We have provisionally concluded that the territorial ambit of the Official Secrets Act 1911 is insufficient to offer adequate protection to sensitive assets abroad. For this reason the territorial ambit of the offences ought to be expanded so that the offences can be committed irrespective of whether the individual who is engaging in the prohibited conduct is a British Officer or subject, so long as there is a "sufficient link" with the United Kingdom.

Provisional conclusion 7

2.175 **The territorial ambit of the offences ought to be expanded so that the offences can be committed irrespective of whether the individual who is engaging in the prohibited conduct is a British Officer or subject, so long as there is a "sufficient link" with the United Kingdom. Do consultees agree?**

The provisions which ease the prosecution's burden

2.176 As we discussed in our analysis of the current law, one of the aims of the Official Secrets Acts 1911 and 1920 was to ease the prosecution's burden in respect of proving certain elements of the offences in the Official Secrets Act 1911.

2.177 For example, section 1(2) of the Official Secrets Act 1911 provides that the prosecution does not need to show that the defendant committed any particular act tending to show a purpose prejudicial to the safety or interests of the State. Notwithstanding that no such act has been proved against them, the defendant may be convicted if, from the circumstances of the case, or from the defendant's conduct, or from their "known character as proved", it *appears* that their purpose was a purpose prejudicial to the safety or interests of the State. Therefore, the prosecution does not need to prove beyond reasonable doubt that the defendant had a purpose prejudicial to the interests of the state. It suffices that it *appears* that the defendant had such a purpose from his or her "known character as

[73] D Ormerod and D Perry (eds), *Blackstone's Criminal Practice* (2017), at B17.16 – B17.17.

proved". One reason why this might be objectionable is that it may introduce a standard of proof less than beyond reasonable doubt. Furthermore, it is generally accepted that deeming provisions such as these have no place in the criminal law.

2.178 By virtue of section 2(1) of the Official Secrets Act 1920 communication with a foreign agent provides evidence of the commission of the offences in section 1 of the Official Secrets Act 1911. In addition, section 2(2) of the Official Secrets Act 1920 provides that a person shall, unless they prove the contrary, be deemed to have been in communication with a foreign agent if they have visited the address of a foreign agent or the name or address of, or any other information regarding a foreign agent has been found in their possession, has been supplied to them, or has been obtained by them from any other person.

2.179 Due to the inherently covert nature of the activity that the Official Secrets Acts 1911 and 1920 are intended to criminalise, proof of such activity can be difficult to come by. As we have explained, this was the reason for the repeal of the Official Secrets Act 1889 and the introduction of the Official Secrets Acts 1911 and 1920.

2.180 It is necessary to consider the extent to which section 2(2) of the Official Secrets Act 1920 impacts upon the presumption of innocence enshrined in Article 6(2) of the European Convention on Human Rights.

2.181 Article 6(2) provides that everyone charged with a criminal offence shall be presumed innocent until found guilty according to law.[74] It is important to point out that such a presumption also exists within the common law. Indeed, it was described by Viscount Sankey as the "golden thread" that runs throughout the common law.[75] The reasoning in this section therefore applies equally to the common law as it does to Article 6(2).

2.182 As both domestic courts and the European Court of Human Rights have confirmed on numerous occasions, Article 6(2) is not an absolute right and can be subject to modifications or limitations so long as these pursue a legitimate aim and satisfy the principle of proportionality.[76]

2.183 In evaluating the extent to which section 2(2) constitutes a disproportionate interference with Article 6(2), it is first necessary to distinguish between the legal burden and the so-called evidential burden. If an evidential burden is placed upon

[74] For discussion, see A Ashworth, B Emmerson and A Macdonald (eds), *Human Rights and Criminal Justice* (3rd ed 2012) ch 15.

[75] *Woolmington v Director of Public Prosecutions* [1935] AC 462, 481.

[76] A Ashworth, B Emmerson and A Macdonald (eds), *Human Rights and Criminal Justice* (3rd ed 2012) pp 670-687.

the defendant, then he or she must adduce sufficient evidence in support of a given proposition. The burden then shifts to the prosecution to disprove that proposition beyond a reasonable doubt. If a legal burden is placed upon the defendant, then he or she must prove on a balance of probabilities a proposition which is essential to the determination of liability. The prosecution is therefore absolved of the responsibility of having to prove this proposition.[77]

2.184 In *Attorney General's Reference (Number 4 of 2002); Sheldrake v Director of Public Prosecutions* Lord Bingham held that Article 6(2) of the European Convention on Human Rights does not outlaw presumptions of law or fact, but does require them to be kept within reasonable limits and mandates that they must not be arbitrary.[78] Lord Bingham listed six factors that are relevant when considering whether a reverse burden infringes the presumption of innocence:

(1) The opportunity given to the defendant to rebut the presumption.

(2) Maintenance of the rights of the defence.

(3) Flexibility in the application of the presumption.

(4) Retention by the court of the power to assess the evidence.

(5) The importance of what is at stake.

(6) The difficulty which a prosecutor may face in the absence of the presumption.[79]

2.185 As we have already explained, section 2(2) of the Official Secrets Act 1920 mandates that a person shall, unless they prove the contrary, be deemed to have been in communication with a foreign agent if they have visited the address of a foreign agent, or the name or address of, or any other information regarding, a foreign agent has been found in their possession, has been supplied to them, or has been obtained by them from any other person.

2.186 If someone visits the address of a foreign agent, the name or address of, or any other information regarding, a foreign agent is found in their possession, has been supplied to them, or has been obtained by them from any other person, then section 2(2) places a burden upon the defendant to prove on the balance of

[77] C Tapper, *Cross and Tapper on Evidence* (12th ed 2010) pp 143-250.

[78] *Attorney General's Reference (Number 4 of 2002); Sheldrake v Director of Public Prosecutions* [2005] 1 AC 264.

[79] *Attorney General's Reference (Number 4 of 2002); Sheldrake v Director of Public Prosecutions* [2005] 1 AC 264, at [21].

probabilities that they have not been in communication with a foreign agent. If the defendant fails to discharge this burden, then they will be presumed to have been in communication with a foreign agent, which in turn provides evidence of commission of one of the offences contained in section 1 of the Official Secrets Act 1911.

2.187 To ensure a Convention compatible interpretation, we believe a court would, if the provision were ever to be challenged, invoke section 3 of the Human Rights Act 1998 to "read down" this provision and interpret it as only imposing an evidential burden. This would mean that the burden to prove beyond reasonable doubt that the defendant had been in communication with a foreign agent would remain on the prosecution. It would not be for the defendant to prove that they had not been in communication with a foreign agent.

2.188 We believe a court would take a similar approach to section 1(2) of the Official Secrets Act 1911. On one reading, this provision absolves the prosecution of having to prove beyond reasonable doubt that the defendant had a purpose prejudicial to the interests of the state. It suffices if the prosecution proves that it *appears* that the defendant had such a purpose from his "known character as proved". To ensure a Convention compatible interpretation of the provision, it is likely that a court would invoke section 3 of the Human Rights Act 1998 and insist on the prosecution proving beyond reasonable doubt that the defendant had a purpose prejudicial to the interests of the state.

2.189 If these provisions were challenged, the courts could achieve a Convention compatible meaning by invoking section 3 of the Human Rights Act 1998. We believe, however, that it would be preferable for the legislation not to contain provisions such as these. We do not underestimate the difficulty in proving the commission of espionage offences, but provisions such as those contained in the Official Secrets Acts 1911 and 1920 are difficult to reconcile with principle. In this regard, it is important to bear in mind that the means of investigating espionage are much more advanced than they were when the Official Secrets Acts 1911 and 1920 were enacted.

Consultation question 5

2.190 **Bearing in mind the difficulties inherent in proving the commission of espionage, do consultees have a view on whether the provisions contained in the Official Secrets Acts 1911 and 1920 intended to ease the prosecution's burden of proof are so difficult to reconcile with principle that they ought to be removed or do consultees take the view that they remain necessary?**

THE OPTIMAL LEGISLATIVE VEHICLE FOR REFORM

2.191 In the previous section, we set out ways the current legislative regime could be amended to make it more effective and to remedy some of the anomalies that seem out of place in the contemporary era. In this section, we evaluate the extent to which it would be preferable for these reforms to form the basis of a new Act. This would entail repealing the Official Secrets Acts 1911-1939 and replacing them with a new, modern statute.

2.192 There are a number of reasons why we believe this approach could be preferable to enacting a series of further amendments to what are already outdated and repeatedly amended statutes:

(1) The titles of the Official Secrets Acts do not accurately convey the distinct purposes of the legislation. The aim of the 1911-1939 Acts is to criminalise those who engage in espionage. As we will discuss in the next chapter, the aim of the 1989 Act is to criminalise the unauthorised disclosure of specified categories of information. Despite the fact they have the same title, the aims of the legislation are distinct. Ideally, this would be demonstrated by their having different titles.

(2) The title of the legislation is obscure and does not necessarily convey its aim. A new act could have a name that reflects the forms of conduct it is intended to criminalise, such as the "Espionage Act".

(3) It could be difficult to amend the existing legislation in the ways we have suggested without making the legislation incoherent and more difficult to comprehend. This would frustrate our aim of ensuring the legislation offers effective protection.

(4) A new Act could be drafted so as to be compliant with the European Convention on Human Rights.

2.193 Further amending the Official Secrets Acts 1911-1939 would be to repeat the errors that were made in the past. As Thomas has argued, the effect of the Official Secrets Acts 1920 and 1939 was to render the Official Secrets Act 1911 incoherent. Further amendments would compound this incoherence.

2.194 The cumulative impact of these factors have led us provisionally to conclude that the optimal solution to the problems we have identified is to repeal the Official Secrets Acts 1911-1939 and replace them with a single, modern statute that is fit for purpose in the modern era. It is important for consultees to bear in mind that the issues we have considered in this chapter are not exhaustive and the contents of any future legislation would need further examination.

Provisional conclusion 8

2.195 **We provisionally conclude that the Official Secrets Acts 1911-1939 ought to be repealed and replaced with a single Espionage Act. Do consultees agree?**

CHAPTER 3
THE OFFICIAL SECRETS ACT 1989

INTRODUCTION

3.1 This chapter analyses the provisions contained within the Official Secrets Act 1989. The aim of this chapter is to explain the current law and evaluate the extent to which there are problems with it. Having set out the problems that have been brought to our attention, this chapter outlines how the law could be reformed and asks for consultees' views on a number of options for reform.

BACKGROUND

3.2 The Official Secrets Act 1989 cannot be understood without first discussing the legislation that preceded it.[1] Prior to the enactment of the Official Secrets Act 1989, section 2 of the Official Secrets Act 1911 criminalised the unauthorised disclosure of any information entrusted to Crown Servants. The Official Secrets Act 1911 is discussed in detail in Chapter 2. The analysis here is confined to the offence that was formerly contained in section 2.

3.3 The main offence in section 2 criminalised the unauthorised communication of official information by any person who held office under Her Majesty. The section criminalised other forms of behaviour. It was an offence for an individual to communicate to an unauthorised person information which was entrusted in confidence to them by any person who held office under Her Majesty or which was obtained as a person who held a contract on behalf of Her Majesty. Other parts of section 2, as amended, made it an offence:

(1) To use information for the benefit of any foreign power.

(2) To communicate information about munitions of war directly or indirectly to a foreign power.

(3) To retain official papers which should be returned.

(4) To fail to take reasonable care of official papers, and

(5) To receive information knowing or having reasonable grounds to believe that it was communicated in contravention of the 1911 Act.

3.4 In 1971, a Departmental Committee under Lord Franks of Headington was appointed by the Home Secretary "to review the operation of section 2 of the Official Secrets Act 1911 and to make recommendations".[2] The Committee included members of both Houses of Parliament and the media. The Committee received a large volume of written and oral evidence.

[1] For discussion see D Williams, *Not in the Public Interest* (1965); Departmental Committee on Section 2 of the Official Secrets Act 1911 (1972) Cmnd 5104, pp 23-27; R Thomas, *Espionage and Secrecy* (1991).

[2] Departmental Committee on Section 2 of the Official Secrets Act 1911 (1972) Cmnd 5104, p 1.

3.5 Section 2 of the Official Secrets Act 1911 was described by the Franks Committee as a "legislative mess".[3] The Franks Committee observed how section 2 was drafted in very wide terms and was highly condensed. The point was made that on one calculation section 2 permitted two thousand differently worded charges to be brought under it.[4]

3.6 The Franks Committee concluded that section 2 of the Official Secrets Act 1911 exhibited two fundamental problems of principle. First, the offence was contained in an Act primarily intended to criminalise spies and traitors. Section 2 was described as a "conspicuous exception" on the basis that it criminalised an individual who may have had no intention to harm their country. It is for this reason the Franks Committee recommended excising the unauthorised disclosure offences from the Official Secrets Act and enacting a separate Official Information Act. Secondly, the Committee concluded that section 2 was "enormously wide" and that any law which impinges upon the freedom of information in a democracy ought to be more tightly drawn. This echoed similar criticisms others had made of section 2.

3.7 The collective weight of the evidence submitted to the Franks Committee led it to conclude that section 2 of the Official Secrets Act 1911 needed to be replaced by a more narrowly drawn provision. The Franks Committee sought to achieve this aim by examining which categories of official information justified the protection of the criminal law. It concluded:

> We believe that most of those who have given evidence to us, and most reasonable people, would accept as a proper basis for the employment of criminal sanctions the unauthorised disclosure of official information which would be likely to cause serious injury to the security of the nation or the case of the people. If criminal sanctions are justified at all, they are justified for this purpose.[5]

3.8 The Franks Committee recommended that only information falling within the following categories ought to be protected by the criminal law, but only if it bore the classification SECRET or DEFENCE-CONFIDENTIAL:

(1) Defence and internal security.

(2) Foreign relations.

(3) Currency and the reserves.[6]

3.9 The Committee recommended that before a decision was taken to institute a prosecution for the disclosure of classified information that fell within one of these

[3] Departmental Committee on Section 2 of the Official Secrets Act 1911 (1972) Cmnd 5104, p 37.

[4] Departmental Committee on Section 2 of the Official Secrets Act 1911 (1972) Cmnd 5104, p 37.

[5] Departmental Committee on Section 2 of the Official Secrets Act 1911 (1972) Cmnd 5104, p 47.

[6] Departmental Committee on Section 2 of the Official Secrets Act 1911 (1972) Cmnd 5104, pp 48-52.

three categories, the responsible Minister should review whether the information was correctly classified and give a certificate to that effect to the court. This certificate would provide conclusive proof that the information was correctly classified and therefore could not be challenged by the defendant.[7]

3.10 The Franks Committee believed that confining criminal liability to classified information would ensure that only unauthorised disclosures that caused serious damage would fall within the ambit of the criminal law.

3.11 In addition, the Committee recommended that the following categories of information ought to be protected by the criminal law, irrespective of classification.

(1) Law and order, for example information likely to be helpful in the commission of a criminal offence.

(2) Papers and minutes of Cabinet and Ministerial Cabinet Committees.

(3) Information given to the Government by private individuals or concerns, whether given by reason of compulsory powers or otherwise, and whether or not given on an express or implied basis of confidence.

(4) Official information used for private gain.[8]

3.12 In a House of Commons debate on 29 June 1973, there was general support for the view that the Franks Committee's proposals were broadly acceptable.[9] No bill, however, was introduced. Despite the fact they were not enacted, the recommendations made by the Franks Committee provided the starting point for subsequent discussions on reform of section 2 of the Official Secrets Act 1911.

3.13 Section 2 was not considered for reform again until the Government published a White Paper in 1978.[10] The recommendations in the White Paper were modelled upon the Frank Committee's recommendations. There were, however, a number of important differences:

(1) The criminal law would not apply to the unauthorised disclosure of papers and minutes of Cabinet meetings and Ministerial Cabinet Committees or to information relating to the currency and reserves.

(2) Greater protection would be given to information relating to individuals and private firms.

(3) The responsible Minister would no longer issue a certificate confirming that the information was appropriately classified. Instead, the Minister would specifically consider whether the disclosure of the information met

7 Departmental Committee on Section 2 of the Official Secrets Act 1911 (1972) Cmnd 5104, pp 60-61.

8 Departmental Committee on Section 2 of the Official Secrets Act 1911 (1972) Cmnd 5104, pp 71-76.

9 *Hansard* (HC),29 June 1973, vol 858, cc 1886-889.

10 Reform of Section 2 of the Official Secrets Act 1911 (January 1978) Cmnd 7285.

the serious injury test, with the Attorney General reviewing the accuracy of this assessment. If the Attorney General agreed, a certificate would be issued, which would be conclusive proof that the unauthorised disclosure was damaging.

3.14 The following year, the new Government introduced a Protection of Official Information Bill into the House of Lords. This was modelled upon the 1978 White Paper. Much of the focus of the debate on the Bill was centred on the failure to introduce freedom of information legislation.[11] In addition, criticisms were made of the fact that the defendant would be unable to challenge the Minister's conclusion that the disclosure was damaging. Finally, there was vociferous criticism of the fact that the Bill criminalised the disclosure of any information that related to security and intelligence irrespective of whether it caused harm. Although the Bill received a second reading, the cumulative effect of these criticisms led the Government to withdraw it.

3.15 In 1988 the Government set out fresh proposals to reform section 2 of the Official Secrets Act 1911. In the White Paper, the Government affirmed its belief that certain categories of information require the protection of the criminal law because of the harm that can be caused by their unauthorised disclosure.[12]

3.16 The Government outlined the criticisms made of section 2 in the following terms:

> The drafting of section 2 is archaic and, in places, obscure. But the central objection is its scope. It penalises the disclosure of *any* information obtained by a person holding office under the Crown or a government contractor in the course of his duties, however trivial the information and irrespective of the harm likely to arise from 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 has 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.[13]

3.17 The Government sought to replace section 2 of the Official Secrets Act 1911 with a provision that was "easily comprehensible, readily applicable by the courts and widely accepted as useful and necessary".[14] To achieve these aims the Government sought to craft a provision that was narrower in scope than section 2. The overarching aim was to ensure that the limited range of circumstances in

[11] *Hansard* (HL), 5 November 1979, vol 402, cc 619-676.

[12] Reform of Section 2 of the Official Secrets Act 1911 (1988) Cm 408.

[13] Reform of Section 2 of the Official Secrets Act 1911 (1988) Cm 408, para 6.

[14] Reform of Section 2 of the Official Secrets Act 1911 (1988) Cm 408, para 13.

which an unauthorised disclosure of official information would constitute a criminal offence would be more clearly defined.[15]

3.18 The White Paper followed many of the recommendations made in the 1978 White Paper. There were, however, a number of significant changes.

(1) The Government accepted the criticisms that were made of the suggestion that a Ministerial certificate ought to be conclusive proof of damage. These criticisms focused on the fact that since there would be no opportunity to challenge the Minister's certificate, an essential element of the offence would not be considered by the courts but would be decided by the Minister alone. It was argued that this could lead to the perception that the certificate was issued as a result of political bias or a fear that a particular disclosure would be embarrassing rather than because it would in fact cause serious injury to the nation's interests. This led the Government to conclude that the issue of damage ought to be considered by the court. The prosecution would have to adduce evidence as to the damage caused and the defence would have the opportunity to present its own evidence as to why the disclosure was not damaging. The burden of proof would therefore operate in the normal way.

(2) A preference was expressed for a concrete and specific test of harm that could be applied by the courts, rather than the broad test proposed by the 1978 White Paper. The Government took the view that the disclosure of different categories of information had the potential to cause different types of harm and that this should be reflected in the test for establishing harm. The Government therefore proposed separate tests of likely harm for the different categories of information to be covered by future legislation. The Government recognised that it could be difficult to prove that the disclosure was in fact damaging. For that reason, the Government suggested that it ought to suffice if the information was of a class or description the disclosure of which would be likely to damage a specified list of interests. The rationale for this change was that it would allow the evidence placed before the court to be less specific.

(3) It was accepted that information relating to security or intelligence should not be given blanket protection, as this had been a major criticism of the 1978 White Paper. To meet this criticism, it was suggested that unless the person who disclosed the information was a member or former member of the security and intelligence agencies or was a notified person, then the prosecution should have to prove that the disclosure was damaging. The reason for this distinction was the Government's belief that disclosures made by members or former members of the security and intelligence agencies carry a credibility which a disclosure made by someone who did not occupy such a position lacks. Additionally, the point was made that those who choose to join the security and intelligence agencies do so knowing about the special and inescapable duty of secrecy that membership of those organisations entails.

[15] Reform of Section 2 of the Official Secrets Act 1911 (1988) Cm 408, para 14.

(4) The Government did not agree with the 1978 White Paper that the unauthorised disclosure of information provided in confidence to Crown servants by companies and private individuals should be an offence in every instance. The Government concluded that since the legislation was only intended to protect information the disclosure of which would seriously harm the public interest, it would not be right to give blanket protection to all information offered in confidence.[16]

3.19 The White Paper concluded with the following statement:

> This White Paper presents a set of proposals the central objective of which is to apply the criminal law to those, and only those, who disclose a limited range of information without authority knowing or having good reason to know that to do so is likely to harm the public interest. The proposals would not apply criminal sanctions to disclosures which are not likely to harm the public interest, nor to anyone who could not reasonably have been expected to foresee the effect of his disclosure.[17]

3.20 During the passage of the Official Secrets Bill, amendments were introduced in both Houses.[18] A number of these amendments sought to insert a public interest defence into the Bill, but they were all rejected. We return to the issue of public interest in Chapter 7. The Bill received the Royal Assent on 11 May 1989 and came into force as the Official Secrets Act 1989 on 1 March 1990.

THE OFFICIAL SECRETS ACT 1989

3.21 This section will analyse the offences contained within the Official Secrets Act 1989. Broadly speaking, the following categories of information fall within the scope of the Official Secrets Act 1989:

(1) Security and intelligence.

(2) Defence.

(3) International relations.

(4) Crime and special investigation powers.

(5) Information entrusted in confidence to or by other states or international organisations.

[16] Reform of Section 2 of the Official Secrets Act 1911 (1988) Cm 408, paras 15-19.

[17] Reform of Section 2 of the Official Secrets Act 1911 (1988) Cm 408, para 77.

[18] *Hansard* (HC), 15 February 1989, vol 147 cc 333-441; 16 February 1989, vol 147 cc 503-610; 22 February 1989, vol 147 cc 1002-1017. *Hansard* (HL), 03 April 1989, vol 505 cc 906-958, 976-997; 18 April 1989, vol 506 cc 698-756; 24 April 1989, vol 506 cc 1065-106.

3.22 Each category of information is protected in a different section of the 1989 Act. For the sake of clarity, each section will be examined in turn.[19]

Section 1 – Security and intelligence

3.23 Section 1 of the Official Secrets Act 1989 applies to different types of officeholder. The elements of the offences differ depending upon the office held by the discloser of the information, which is why we examine them separately.

Members of the security and intelligence services and those who are notified that they are subject to the Act

3.24 Section 1(1) applies to a person who is, or has been, a member of the security and intelligence services, or a person notified that they are subject to the provisions of the 1989 Act.[20] Such a person commits a criminal offence, if without lawful authority, they disclose any information, document or other article relating to security or intelligence. The information, document or other article must have been in that person's possession by virtue of their position as a member of any of the security and intelligence services or in the course of their work whilst the notification was in force. Importantly, section 13(1) provides that "disclose" and "disclosure" in relation to a document or other article includes parting with possession of it. The term therefore encompasses more than giving information to someone else, but also includes leaving it for someone else to find.

3.25 Unlike almost all of the other offences in the 1989 Act, commission of the offence contained in section 1(1) is not contingent upon proof that the disclosure was damaging. As has already been examined briefly, two reasons for this were advanced in the White Paper. First, "because members of the services know that their membership carries with it a special and inescapable duty of secrecy about their work". Secondly, because such disclosures "carry a credibility which the disclosure of the same information by any other person does not, and because they reduce public confidence in the services' ability and willingness to carry out their essentially secret duties effectively and loyally".[21]

3.26 By virtue of section 1(6), notification that a person is subject to the 1989 Act has effect by way of a notice in writing served on them by a Minister of the Crown. Such a notice will be served if, in the Minister's opinion, "the work undertaken by the person in question is or includes work connected with the security and

[19] For some early analysis of the legislation, see S Palmer, "Tightening secrecy law: the Official Secrets Act 1989" (1990) *Public Law* 243; J Griffith, "The Official Secrets Act 1989" (1989) *Journal of Law and Society* 273; S Palmer, "In the interests of the state: the government's proposals for reforming section 2 of the Official Secrets Act 1911" (1988) *Public Law* 523.

[20] By virtue of section 1(9), the term "security and intelligence" means the work of, or in support of, the security and intelligence services or any part of them, and references to information relating to security or intelligence includes references to information held or transmitted by those services or by person in support of, of any part of, them.

[21] Reform of Section 2 of the Official Secrets Act 1911 (1988) Cm 408, para 41.

intelligence services and its nature is such that the interests of national security require that he should be subject to the provisions of that subsection".[22]

3.27 By virtue of section 1(5) if the defendant is or was a member of the security and intelligence services or a notified person, it is a defence that, at the time of the alleged offence, the defendant did not know, and had no reasonable cause to believe, that the information, article or document in question related to security or intelligence.

Crown servants and government contractors

3.28 By virtue of section 1(3) a person who is, or has been, a Crown servant or government contractor is guilty of an offence if without lawful authority they make a damaging disclosure of any information, document or other article relating to security or intelligence which is in their possession by virtue of their position as a Crown servant or government contractor.[23] Crown servant is a term defined in section 12(1) of the Official Secrets Act 1989. It is defined in the following terms:

(1) a Minister of the Crown;

(2) a member of the Scottish Executive or a junior Scottish Minister;

(3) the First Minister for Wales, a Welsh Minister appointed under section 48 of the Government of Wales Act 2006, the Counsel General to the Welsh Assembly Government or a Deputy Welsh Minister;

(4) a person appointed under section 8 of the Northern Ireland Constitution Act 1973;

(5) any person employed in the civil service of the Crown, including Her Majesty's Diplomatic Service, Her Majesty's Overseas Civil Service, the civil service of Northern Ireland and the Northern Ireland Court Service;

(6) any member of the naval, military or air forces of the Crown, including any person employed by an association established for the purposes of Part XI of the Reserve Forces Act 1996;

(7) any constable and any other person employed or appointed in or for the purposes of any police force (including the Police Service of Northern Ireland and the Police Service of Northern Ireland Reserve) or an National Crime Agency special;

(8) any person who is a member or employee of a prescribed body or a body of a prescribed class and either is prescribed for the purposes of this paragraph or belongs to a prescribed class of members or employees of any such body;

[22] By virtue of section 1(7) a notification remains in force for five years beginning on the day on which it is served and may be renewed by further notices for periods of five years at a time. Section 1(8) provides that a notification may be revoked by a further notice in writing by the Minister to the person concerned as soon as, in the Minister's opinion, the work undertaken by that person ceases to fall within section 1(6).

[23] Section 12 defines the terms "Crown servant" and "government contractor".

(9) any person who is the holder of a prescribed office or who is an employee of such a holder and either is prescribed for the purposes of this paragraph or belongs to a prescribed class of such employees.

3.29 Section 12(2) defines the term "government contractor" as:

> Any person who is not a Crown servant but who provides, or is employed in the provision of, goods or services—
>
> > for the purposes of any Minister or person mentioned in [section 12(1)] or of any office-holder in the Scottish Administration, of any of the services, forces or bodies mentioned in [section 12(1)] or of the holder of any office prescribed under [section 12(1)];
> >
> > under an agreement or arrangement certified by the Secretary of State as being one to which the government of a State other than the United Kingdom or an international organisation is a party or which is subordinate to, or made for the purposes of implementing, any such agreement or arrangement.

3.30 By virtue of section 1(4), there are three ways a disclosure may be damaging:

(1) it causes damage to the work of, or to any part of, the security and intelligence services; or

(2) it is of information or a document or another article which is such that its unauthorised disclosure would be likely to cause such damage; or

(3) it is of information which falls within a class or description of information, documents or other articles the unauthorised disclosure of which would be likely to have that effect.

3.31 Although the legislation is ambiguous, it is submitted that the terms "such damage" and "that effect" must refer to damage being caused to the work of, or any part of, the security and intelligence services. There is no further definition, however, of the term "damage".[24]

3.32 As has already been touched upon briefly, the Government recognised that the requirement to prove harm could hinder the ability to initiate prosecutions. The White Paper contained the following explanation as to why this might be the case:

> In order to prove the truth of the information at present, and in order to satisfy the test of harm if the Government's proposal is adopted, evidence may need to be adduced which involves a disclosure which

[24] It has been suggested that proof of the objective risk of damage is insufficient to constitute the offence. See D Ormerod and D Perry (eds), *Blackstone's Criminal Practice* (2017), at B9.45.

> is as harmful as or more harmful than the disclosure which is the subject of the prosecution.[25]

3.33 The Government expressed the view that it would be deeply undesirable for those who disclosed information which caused damage to the security and intelligence services to "be able to do so with impunity, simply by reason of the sensitivity of the subject matter".[26]

3.34 To preclude such a scenario from arising, the legislation provides that damage can be satisfied by categories (2) and (3) above. The Government expressed the view that:

> This would allow the arguments before the court to be less specific. The prosecution would have to satisfy the court that a particular disclosure was of a certain class or description, and that disclosure of information of that class or description was likely to damage the operation of the services.[27]

3.35 Whether this aspect of the legislation fulfils the aims intended of it is an issue that we return to later in this chapter.

3.36 By virtue of section 1(5), it is a defence that the Crown servant or government contractor did not know, and had no reasonable cause to believe, that the disclosure would be damaging within the meaning of section 1(3).

Section 2 – Defence

3.37 The offence in section 2 makes it an offence for someone who is or has been a Crown servant or government contractor without lawful authority to make a damaging disclosure of any information, document or other article relating to defence which is or has been in their possession by virtue of their position as such.[28] The offence in section 2 shares many characteristics with its counterpart in section 1(3). The commission of this offence, however, is always contingent upon proof that the disclosure was damaging.

3.38 Section 2 provides that a disclosure is damaging if:

(1) it damages the capability of, or any part of, the armed forces of the Crown to carry out their tasks or leads to loss of life or injury to members of those forces or serious damage to the equipment of installations of those forces; or

[25] Reform of Section 2 of the Official Secrets Act 1911 (1988) Cm 408, para 39.

[26] Reform of Section 2 of the Official Secrets Act 1911 (1988) Cm 408, para 39.

[27] Reform of Section 2 of the Official Secrets Act 1911 (1988) Cm 408, para 40.

[28] By virtue of section 2(4), the term "defence" means: the size, shape, organisation, logistics, order of battle, deployment, operations, state of readiness and training of the armed forces of the Crown; the weapons, stores or other equipment of those forces and the invention, development, production and operation of such equipment and research relating to it; defences policy and strategy and military planning and intelligence; and plans and measures for the maintenance of essential supplies and services that are or would be needed in time of war.

(2) it endangers the interests of the United Kingdom abroad, seriously obstructs the promotion or protection by the United Kingdom of those interests or endangers the safety of British citizens abroad; or

(3) it is of information or of a document or article which is such that its unauthorised disclosure would be likely to have any of those effects.

3.39 Section 2(3) provides that it is a defence for a person charged with an offence under section 2 to prove that at the time of the alleged offence, they had no reasonable cause to believe that the information, document or article in question related to defence or that its disclosure would be damaging.

Section 3 – International relations

3.40 The offence in section 3 makes it an offence for a person who is or has been a Crown servant or government contractor without lawful authority to make a damaging disclosure of the following categories of information:

(1) any information, document or other article relating to international relations; or

(2) any confidential information, document or other article which was obtained from a state other than the United Kingdom or from an international organisation.[29]

3.41 Section 3(2) provides that a disclosure is damaging if:

(1) it endangers the interests of the United Kingdom abroad, seriously obstructs the promotion or protection by the United Kingdom of those interests, or endangers the safety of British citizens abroad; or

(2) it is of information, of a document or article which is such that its unauthorised disclosure would be likely to have those effects.

3.42 In the White Paper the Government expressed the view that any unauthorised disclosure of information that has been obtained in confidence from another government or international organisation is intrinsically harmful, as it undermines the United Kingdom's international standing and could have a detrimental impact upon the willingness to share information with the United Kingdom.[30]

3.43 In relation to confidential information which was obtained from a state other than the United Kingdom, section 3(3) provides that the confidential status of the information or its nature and contents may be sufficient to establish that the unauthorised disclosure of the information was damaging. Section 3(6) clarifies that any information, document or article obtained from a state or organisation will be deemed to be confidential if the terms on which it was obtained require it to be

[29] By virtue of section 3(5), the term "international relations" means, "the relations between States, between international organisations or between one or more States and one or more such organisations and includes any matter relating to a State other than the United Kingdom or to an international organisation which is capable of affecting the relations of the United Kingdom with another State or with an international organisation.

[30] Reform of Section 2 of the Official Secrets Act 1911 (1988) Cm 408, paras 27-28.

held in confidence or the circumstances in which it was obtained make it reasonable for the state or organisation to expect that it would be so held.

3.44 Section 3(5) provides that it is a defence for a person charged with an offence under section 3 to prove that at the time of the alleged offence they did not know and had no reasonable cause to believe that the information fell within the scope of section 3(1) or that its disclosure would be damaging.

Section 4 – Crime and special investigation powers

3.45 Section 4 of the Official Secrets Act 1989 makes it an offence for a Crown servant or government contractor to disclose, without lawful authority, any information, document or other article that falls within one of the following categories:

(1) information the disclosure of which results in the commission of another offence; or

(2) information the disclosure of which facilitates an escape from legal custody or the doing of any other act prejudicial to the safekeeping of persons in legal custody; or

(3) information the disclosure of which impedes the prevention or detection of offences or the apprehension or prosecution of suspected offenders.

3.46 It suffices if the information was such that its unauthorised disclosure was likely to have one of these effects.

3.47 It is a defence for a person charged with an offence under this section to prove that at the time of the alleged offence they did not know, and had no reasonable cause to believe, that the disclosure would have the effects listed above.

3.48 In addition, section 4(5) provides that it is a defence for a person charged with an offence under this section to prove that they did not know and had no reasonable cause to believe that the information, document or article in question fell within the scope of the section.

3.49 In terms of the offences, section 4(3)(a) makes it an offence to disclose without authorisation any communication obtained under a warrant issued under section 2 of the Interception of Communications Act 1985 or section 5 of the Regulation of Investigatory Powers Act 2000.[31] This section also makes it an offence to disclose without lawful authority any information relating to the obtaining of information by reason of any interception under these provisions and any document of other article which is or has been used or held for use in, or has been obtained by reason of, any such interception.

3.50 Section 4(3)(b) makes it an offence to disclose without lawful authority any information obtained under a warrant issued under section 3 of the Security

[31] Schedule 10, Part 2 of the Investigatory Powers Act 2016 will, when in force, amend section 4(3) of the Official Secrets Act 1989 to remove reference to the Regulation of Investigatory Powers Act 2000 and replace it with reference to the relevant provisions contained in the Investigatory Powers Act.

Service Act 1989 or under section 5 of the Intelligence Services Act 1994 or by an authorisation given under section 7 of that Act. This section also makes it an offence to disclose without lawful authority any document or other article which is or has been used or held for use, or has been obtained under either of these provisions.

3.51 Finally, section 4(3)(c), which was inserted by the Investigatory Powers Act 2016, makes it an offence, when commenced, to disclose without lawful authority any information obtained under a warrant issued under Chapter 1 of Part 2 or Chapter 1 of Part 6 of the Investigatory Powers Act 2016. This section also makes it an offence to disclose without lawful authority any document or other article which is or has been used or held for use in, or has been obtained by reason of, the obtaining of information under such a warrant.

3.52 Commission of these offences does not depend upon proof of damage. In the White Paper, the Government explained that in relation to those categories not inserted by subsequent legislation, it was self-evident that the relevant disclosure would cause harm to the public interest and no separate test of damage was necessary.[32]

Section 5 – Information resulting from unauthorised disclosures or entrusted in confidence

3.53 In the White Paper, the Government explained that what justifies the criminalisation of certain unauthorised disclosures is the harm they cause to the public interest. The Government took the view that an unauthorised disclosure committed by a newspaper could be just as harmful as the disclosure of the same information by a Crown servant.[33] It was for this reason the Government concluded that it would be insufficient if the criminalisation of harmful disclosures was limited to Crown servants. It elaborated as follows:

> The objective of official secrets legislation is not to enforce Crown service discipline – that is not a matter for the criminal law – but to protect information which in the public interest should not be disclosed. Such protection would not be complete if it applied to disclosure only by certain categories of person. The Government accordingly proposes that the unauthorised disclosure by any person of information in the specified categories in circumstances where harm is likely to be caused should be an offence.[34]

3.54 The White Paper did recognise, however, a distinction between the liability of Crown servants and government contractors and others who do not hold such positions. The Government concluded that it was reasonable to assume that a Crown servant is aware that the unauthorised disclosure of certain categories of information may be harmful to the public interest. Such an assumption cannot,

[32] Reform of Section 2 of the Official Secrets Act 1911 (1988) Cm 408, paras 52-53.

[33] Reform of Section 2 of the Official Secrets Act 1911 (1988) Cm 408, para 54.

[34] Reform of Section 2 of the Official Secrets Act 1911 (1988) Cm 408, para 54.

according to the White Paper, be made about those who are not Crown servants.[35]

3.55 The Government stated that there ought to be a presumption that someone who is not a Crown servant is unaware that disclosure of information might cause harm to the public interest. Therefore in cases involving someone who is not a Crown servant, the White Paper concluded that there ought to be a burden on the prosecution to prove not only that the disclosure would be likely to result in harm, but also that the person who made the disclosure knew, or could reasonably have been expected to know, that harm would be likely to result.

3.56 These conclusions are reflected in section 5 of the Official Secrets Act 1989. Unlike the other offences, the offence in section 5 can be committed by individuals who are not Crown servants, government contractors or notified persons. This offence applies to any information, document or other article that is protected against disclosure by one of the foregoing provisions in the Official Secrets Act 1989.

3.57 Section 5 is applicable if any information, document or other article comes into another person's possession in one of the following scenarios:

(1) it has been disclosed (whether to him or her, or another) by a Crown servant or government contractor without lawful authority; or

(2) it has been entrusted to him or her by a Crown servant or government contractor in terms requiring it to be held in confidence or in circumstances in which the Crown servant or government contractor could reasonably expect that it would be so held; or

(3) It has been disclosed (whether to him or her, or another) without lawful authority by a person to whom it was entrusted as mentioned in (2).

3.58 An offence is committed if the person into whose possession the information, document or other article has come discloses it without lawful authority, knowing or having reasonable cause to believe that it is protected against disclosure by the 1989 Act and that it came into their possession as a result of one of the three scenarios above.

3.59 In addition, scenarios (1) to (3) above do not refer to information disclosed, or entrusted, by notified persons. This suggests that an individual does not commit an offence if they further disclose information that has been supplied to them by a notified person who was acting without lawful authority. So far as we can ascertain, no explanation is provided as to why this might be the case.

3.60 By virtue of section 5(4), a person does not commit an offence if the information was disclosed to them by a government contractor unless the disclosure was made by a British citizen or the disclosure took place in the United Kingdom, Channel Islands, in the Isle of Man or a colony. Although the legislation is ambiguous, it seems to be the case that if the information was disclosed by a Crown servant, then an offence will be committed irrespective of whether the

[35] Reform of Section 2 of the Official Secrets Act 1911 (1988) Cm 408, para 55.

Crown servant was a British citizen or the disclosure took place in the United Kingdom. There is no explanation given for why government contractors ought to be treated differently from Crown servants in this respect.

3.61 As with the other offences (apart from the offences in section 1(1) and 4(3)), the offence is section 5 is only committed if the disclosure is damaging. In addition, the legislation explicitly states that the defendant must make the disclosure knowing or having reasonable cause to believe that it would be damaging. The question of damage is therefore an element of the offence, rather than a defence that can be invoked by the defendant.

3.62 Importantly, by virtue of section 5(6), a person also commits an offence if without lawful authority they disclose any information, document or other article which they know, or have reasonable cause to believe, has come into their possession as a result of a contravention of section 1 of the Official Secrets Act 1911. Commission of this offence does not depend upon proof of damage.

3.63 Finally, by virtue of section 8(4), a person who has in their possession or under their control any document or other article which it would be an offence contrary to section 5 for them to disclose without lawful authority, commits an offence if they do any of the following:

(1) Fails to comply with an official direction for its return or disposal.

(2) Fails to take such reasonable care to prevent its unauthorised disclosure, provided the information has been supplied on terms requiring it to be held in confidence.

3.64 The term "official direction" is defined in section 8(9) as "a direction duly given by a Crown servant or government contractor or by or on behalf of a prescribed body or a body of a prescribed class". By virtue of section 14(2) no order made under this provision will have effect unless approved by both Houses of Parliament.[36]

Section 6 – Information entrusted in confidence to other states or international organisations

3.65 Section 6 of the Official Secrets Act 1989 applies to any information, document, or other article which:

(1) Relates to security or intelligence, defence or international relations; and,

(2) Has been communicated in confidence by or on behalf of the United Kingdom to another state or to an international organisation.[37]

[36] This power has been exercised once. Schedule 3 to the Official Secrets Act 1989 (Prescription) Order 1990/200 added the Civil Aviation Authority to this list.

[37] By virtue of section 6(5), information, a document or article are communicated in confidence if communicated on terms requiring it to be held in confidence or in circumstances in which the person communicating it could reasonably expect that it would be so held.

(3) Has come into a person's possession as a result of having been disclosed without the authority of that state of organisation or, in the case of the latter, a member of it.

3.66 It is an offence for a person to make a damaging disclosure of such information knowing or having reasonable cause to believe that it falls within one of the above categories, that it has come into their possession in the way described and that its disclosure would be damaging.

3.67 Importantly, by virtue of section 6(3), a person does not commit an offence contrary to this section if the information, document or article is disclosed by them with lawful authority or has previously been made available to the public with the authority of the state of organisation concerned or, in the case of the latter, a member of it.

3.68 By virtue of section 8(6), a person who has in their possession or under their control any document or other article which it would be an offence contrary to section 6 for them to disclose without lawful authority, commits an offence if they do any of the following:

(1) Fails to comply with an official direction for its return or disposal.

(2) Fails to take such reasonable care to prevent its unauthorised disclosure, provided the information has been supplied on terms requiring it to be held in confidence.

3.69 The term "official direction" is defined in section 8(9) as "a direction duly given by a Crown servant or government contractor or by or on behalf of a prescribed body or a body of a prescribed class". By virtue of section 14(2) no order made under this provision will have effect unless approved by both Houses of Parliament.[38]

The territorial ambit of the offences

3.70 By virtue of section 15(1) of the Official Secrets Act 1989, a British Citizen or Crown servant will commit an offence contrary to the Official Secrets Act 1989 if without authorisation they disclose information outside of the United Kingdom.[39]

3.71 When the Franks Committee examined the territorial ambit of the offence that was then contained in section 2 of the Official Secrets Act 1911, it concluded that, "It seems rights that….the servant of the Crown and the subject of the Crown should take with him everywhere in the world his duty under the Act to protect secrets of the State".[40]

3.72 An offence contrary to the Official Secrets Act 1989 may therefore still be committed despite the fact the person who disclosed the information in question

[38] This power has been exercised once. Schedule 3 to the Official Secrets Act 1989 (Prescription) Order 1990/200 added the Civil Aviation Authority to this list.

[39] This does not extend to the offences in sections 8(1), 8(4) and 8(5) of the Official Secrets Act 1989.

[40] Departmental Committee on Section 2 of the Official Secrets Act 1911 (1972) Cmnd 5104, pp 97-98.

was outside the jurisdiction at the time they did so.[41] The person who disclosed the information outside of the United Kingdom must, however, have been a British citizen and/or a Crown servant. If he or she was not a British citizen and/or a Crown servant, then no offence is committed.

3.73 This remains the case even if the individual who disclosed the information without lawful authority was a notified person and therefore had access to information that relates to security and intelligence. Therefore a person who is notified and who, when no longer in the United Kingdom, discloses information that falls within the scope of the Official Secrets Act 1989 without authorisation will not commit an offence unless they are also a British citizen or Crown servant, even if that disclosure caused or was likely to cause damage within the meaning of the 1989 Act.

THE STRICT LIABILITY NATURE OF THE OFFENCES

3.74 The offences are, on their face, offences of strict liability (subject to the prosecution proving that the conduct involved in making a disclosure was intentional). This means that there is no need for the prosecution to prove that the person who disclosed the information in question had a particular state of mind as to the type of information being disclosed or the consequences of disclosing it when they did so. For example, to be guilty of an offence contrary to section 2(1) it suffices that the defendant made a damaging disclosure of information relating to the defence of the United Kingdom. The legislation does not state that the prosecution must prove that the defendant, for example, intended to make a damaging disclosure or was reckless as to whether the disclosure might be damaging.

3.75 It is not strictly accurate, however, to characterise the offences as offences of strict liability. This is because each of the offences in sections 1 – 3 of the Official Secrets Act 1989 contains a defence for the defendant to prove that at the time of the alleged offence, they did not know and had no reasonable cause to believe that the information, document or article in question related to a protected category of information and/or that its disclosure would be damaging.

3.76 The impact of this defence on the offences was analysed extensively by the Court of Appeal in *Keogh*.[42] In *Keogh*, the appellant was a Crown servant employed in the communications centre in Whitehall. He acquired possession of a highly confidential letter between the Prime Minister and the President of the United States concerning political, diplomatic and defence issues regarding the policy of the governments of both the United Kingdom and the United States of America in Iraq. The appellant photocopied the letter and showed it to an individual employed as a political researcher for a Member of Parliament who strongly opposed the Iraq War. The appellant was later charged with committing offences contrary to sections 2 and 3 of the Official Secrets Act 1989.

3.77 The issues for the Court of Appeal were, first, whether the trial judge was correct to conclude that the defendant bore the legal burden of proving that he did not know and had no reasonable cause to believe that his disclosure of protected

[41] For discussion, see M Hirst, *Jurisdiction and the Ambit of the Criminal Law* (2003), p 222.

[42] *R v Keogh* [2007] EWCA Crim 528; [2007] 1 WLR 1500.

information would be damaging and, secondly, whether the imposition of such a legal burden upon the defendant was compatible with Article 6(2) of the European Convention on Human Rights.

3.78 Lord Phillips, the then Lord Chief Justice, held that it is not accurate to state that the offences created by the Official Secrets Act 1989 are committed regardless of any other aspect of the defendant's state of mind. He stated that:

> In reality the offence will not be committed if the defendant did not know and had no reasonable cause to believe in the existence of the ingredients of the offence as defined in sections 2(3) and 3(4) respectively. In practice therefore the analysis of the defendant's alleged criminality requires attention to be given to his state of mind at the moment when the intentional disclosure took place. In the words of sections 2(3) and 3(4) his knowledge, or whether he has reasonable cause to believe in the features identified in these sections, will almost inevitably, or at least very often, be in issue.[43]

3.79 Lord Phillips then observed that if the trial judge was correct to conclude that the provisions in question do impose a legal burden, then the defendant would be required to disprove a substantial ingredient of the offence.[44] A jury could therefore convict a defendant despite entertaining reasonable doubt as to whether they knew or had reasonable cause to believe that the document in question related to the category of information in question and/or that its disclosure would be damaging. This means a jury could convict the defendant despite there being no mental element attaching to either the consequence or circumstance elements of the offence.

3.80 Two factors led the Court of Appeal to conclude that the offences include a mental element that the prosecution is required to establish and the defendant would then be required to disprove. First, the offence in section 5 of the Official Secrets Act 1989 makes knowledge of the material elements of the offence, or reasonable cause to believe they exist, an explicit element of the offence that must be proven by the prosecution. Secondly, the White Paper stated that it would be wrong to criminalise the unauthorised disclosure of information unless the discloser knows or could reasonably be expected to know that the disclosure would be likely to cause harm. This caused Lord Phillips to observe that, "This makes it plain that there was no intention to make disclosure criminal unless the discloser knew, or could reasonably be expected to know, that the disclosure would cause harm".[45]

3.81 As a result of the Court of Appeal's judgment, in every case (other than those involving the offence in sections 1(1)), it is for the prosecution to prove beyond reasonable doubt that the defendant knew or had reasonable cause to believe that the information in question fell within a category encompassed by the Official Secrets Act 1989 and that he or she knew or had reasonable cause to believe that its disclosure would be damaging. This means that a mental element

[43] *R v Keogh* [2007] EWCA Crim 528; [2007] 1 WLR 1500 at [19].

[44] *R v Keogh* [2007] EWCA Crim 528; [2007] 1 WLR 1500 at [20].

[45] *R v Keogh* [2007] EWCA Crim 528; [2007] 1 WLR 1500 at [23].

attaches to both the consequence element of the offence, namely knowledge or reasonable cause to believe that the disclosure would be damaging, and the circumstance element, that the defendant knew or had a reasonable cause to believe that the information in question fell within a category encompassed by the Official Secrets Act 1989

3.82 The fault element "belief" has been defined by the Court of Appeal in *Hall* in the following terms:

> Belief, or course, is something short of knowledge. It may be said to be the state of mind of a person who says to himself: 'I cannot say for certain that [the circumstance exists] but there can be no other reasonable conclusion in the light of all the circumstances, in the light of all that I have heard and seen.[46]

3.83 In relation to whether placing the burden to disprove an essential element of the offence contravened Article 6(2), Lord Phillips held that it was insufficient to state that a Crown servant can be presumed to appreciate the consequences of disclosure. Lord Phillips held that the crucial question was whether the reverse burden was necessary for the effective operation of the offences.[47]

3.84 It was observed that it might be very difficult for the prosecution to prove that the defendant knew that the disclosure would be damaging. Lord Phillips held, however, that this difficulty is mitigated by the fact that it suffices for the prosecution to prove that the defendant had reasonable cause to believe that the information had the relevant characteristics and that its disclosure was likely to be damaging.[48]

3.85 What makes this a more manageable task for the prosecution, according to the court, is that this evaluation does not depend upon the subjective knowledge of the defendant, but rather upon an assessment of objective fact. Due to the fact that the prosecution will have access to the details of the defendant's service as a Crown servant or government contractor, Lord Phillips held that this should enable the prosecution to prove that they had reasonable cause to appreciate the relevant facts.[49]

3.86 The Court of Appeal cited two other relevant factors.[50] First, the prosecution is likely to be confronted by an even more difficult task in establishing the offence in section 5 of the Official Secrets Act 1989, given that it does not apply to Crown servants or government contractors. Secondly, in *R v Director of Public Prosecutions, ex parte Kebilene* the House of Lords used section 3 of the Human Rights Act 1998 to interpret section 118(5) of the Terrorism Act 2000 as only

[46] *R v Hall* (1985) 81 Cr App R 260, 264. For discussion, see D Ormerod and K Laird, *Smith and Hogan's Criminal Law* (14th ed 2015), p 143. A P Simester, J R Spencer, F Stark, G R Sullivan, G J Virgo, *Simester and Sullivan's Criminal Law* (6th ed 2016), p 157.

[47] *R v Keogh* [2007] EWCA Crim 528; [2007] 1 WLR 1500 at [26].

[48] *R v Keogh* [2007] EWCA Crim 528; [2007] 1 WLR 1500 at [29].

[49] *R v Keogh* [2007] EWCA Crim 528; [2007] 1 WLR 1500 at [29].

[50] *R v Keogh* [2007] EWCA Crim 528; [2007] 1 WLR 1500 at [31]-[32].

imposing an evidential burden upon the defendant.[51] The point was made on behalf of the defendant that it was unclear why the relevant provisions in the Official Secrets Act 1989 could not be interpreted in the same way.

3.87 The cumulative weight of these factors led the Court of Appeal to conclude that the Official Secrets Act 1989 can operate effectively without placing a legal burden upon the defendant. To place such a burden upon the defendant would be "disproportionate and unjustifiable".[52] The court therefore invoked section 3 of the Human Rights Act 1998 to interpret the relevant provisions in the Official Secrets Act 1989 as only imposing an evidential burden upon the defendant.

3.88 It is for this reason that it is not quite accurate to characterise the relevant offences in the Official Secrets Act 1989 as being offences of strict liability. Nevertheless, fault is not incorporated explicitly within the terms of the offences. The offences are not offences of knowledge. Knowledge is a purely subjective standard and imposes a high threshold of fault.[53] As the Court of Appeal acknowledged, imposing such a high threshold would make it very difficult for the prosecution to discharge its evidential burden.[54]

3.89 In *Keogh,* Lord Phillips stated that it sufficed if the prosecution could prove that the defendant had reasonable cause to believe that the information fell within a protected category and that its disclosure would be damaging without inviting the jury to engage in a subjective assessment of the defendant's state of mind.[55] The court therefore adopted a wholly objective interpretation of this element.

3.90 As a final point, it is necessary to point out that by virtue of section 7(4) of the Official Secrets Act 1989, it is a defence for a person who is charged with committing an offence contrary to the Official Secrets Act 1989 to prove that at the time of the alleged offence, they believed that they had lawful authority to make the disclosure in question and had no reasonable cause to believe otherwise. Although not considered in *Keogh*, presumably the same reasoning the Court of Appeal adopted in relation to the defences in the other sections of the legislation would be applicable to this defence. Assuming this is correct, an additional burden would be placed upon the prosecution to prove that the defendant did not have a reasonable cause to believe that the disclosure was authorised if that defence is pleaded. Presumably this would also be an objective enquiry, in keeping with *Keogh.*

SAFEGUARDING OF INFORMATION

3.91 Section 8 provides that a Crown servant or government contractor commits an offence if, by virtue of their position as such, they have in their possession or under their control any document or other article which it would be an offence to disclose without lawful authority and:

[51] *R (Kebilene) v Director of Public Prosecutions* [2000] 2 AC 326; [1999] 3 WLR 972.

[52] *R v Keogh* [2007] EWCA Crim 528; [2007] 1 WLR 1500 at [33].

[53] For discussion, see D Ormerod and K Laird, *Smith and Hogan's Criminal Law* (14th ed 2015), pp 141-143. A P Simester, J R Spencer, F Stark, G R Sullivan, G J Virgo, *Simester and Sullivan's Criminal Law* (6th ed 2016), p 157.

[54] *R v Keogh* [2007] EWCA Crim 528; [2007] 1 WLR 1500 at [29].

[55] *R v Keogh* [2007] EWCA Crim 528; [2007] 1 WLR 1500 at [29]-[30].

(1) being a Crown servant they retain the document or article contrary to their official duty; or

(2) being a government contractor, they fail to comply with an official direction for the return or disposal of the document or article; or

(3) being a Crown servant or a government contractor, they fail to take such care to prevent the unauthorised disclosure of the document or article as a person in their position may reasonably be expected to take.[56]

3.92 Importantly, section 8 does not apply to an individual who was formerly a Crown servant. Therefore, such an individual is under no obligation to safeguard information they have in their possession a result of their former employment. This could be problematic if an individual deliberately or inadvertently retains information relating to their former employment and fails to maintain its security. This risk is even greater in the digital era than it was when the 1989 Act was enacted.

3.93 Section 8(2) provides that it is a defence for a Crown servant to prove that at the time of the alleged offence, they believed that they were acting in accordance with their official duty and had no reasonable cause to believe otherwise.

3.94 Section 6(6) makes it an offence to disclose any official information, document, or other article which can be used for the purpose of obtaining access to any information, document or other article that is protected against disclosure by the Official Secrets Act 1989. For the purposes of this offence, a person discloses information or a document or other article if they have possessed it by virtue of their position as a Crown servant or government contractor. Alternatively, a person commits an offence if they know or has reasonable cause to believe that a Crown servant or government contractor has or had possessed it by virtue of their position as such.

AUTHORISED DISCLOSURES

3.95 The Official Secrets Act 1989 only criminalises unauthorised disclosures. Section 7 sets out when a disclosure will be authorised. Distinctions are made in the legislation between disclosures made by current Crown servants, Government contractors, and former Crown servants.

Current Crown servants and notified persons

3.96 A Crown servant or notified person makes an authorised disclosure under section 7(1) if, and only if, it is made in accordance with their official duty. There is no definition in the legislation of "official duty". The legislation does not, on its face, provide a mechanism that facilitates current Crown servants or notified persons who wish to seek official authorisation to make a disclosure. Stakeholders have confirmed, however, that there is a formal process for seeking authorisation that is incorporated in the staff contracts of members of the security and intelligence agencies for the purposes of the duty of confidentiality contained in those

[56] By virtue of section 8(4) of the Official Secrets Act 1989, references to a Crown servant includes any person in whose case a notification for the purposes of section 1(1) is in force.

contracts, and that authorisations by means of these process are regarded as operative also for the purposes of the Official Secrets Act 1989.

Government contractors

3.97 A disclosure made by a government contractor is made with lawful authority under section 7(2) if, and only if, it is made in accordance with an official authorisation or for the purposes of the functions by virtue of which they are a government contractor and without contravening an official restriction. By virtue of section 7(5) the terms "official authorisation" and "official restriction" mean:

> An authorisation or restriction duly given or imposed by a Crown servant or government contractor or by or on behalf of a prescribed body or a body of a prescribed class.

3.98 This is subject to section 7(6), which provides that an "official authorisation" includes "an authorisation duly given by or on behalf of the State concerned, or in the case of an organisation, a member of it."

3.99 The Secretary of State has the power to make a body a "prescribed body" by way of secondary legislation. By virtue of Schedule 2 of the Official Secrets Act 1989 (Prescription) (Amendment) Order 2003/1918, the Civil Aviation Authority and the Investigatory Powers Tribunal are both prescribed bodies for the purposes of the this section.

Former Crown servants

3.100 A disclosure made by any other person, such as someone who was formerly a member of the security and intelligence services or formerly a Crown servant, is made with lawful authority under section 7(3) in two instances. First, if it is made to a Crown servant for the purposes of their functions as such. Secondly, if it is in accordance with an official authorisation.

3.101 In *Shayler,* the House of Lords described the process by which a former Crown servant can seek authorisation to make a disclosure in the following terms:

> As already indicated, it is open to a former member of the service to seek authorisation from his former superior or the head of the service, who may no doubt seek authority from the secretary to the cabinet or a minister. Whoever is called upon to consider the grant of authorisation must consider with care the particular information or document which the former member seeks to disclose and weigh the merits of that request bearing in mind (and if necessary taking advice on) the object or objects which the statutory ban on disclosure seeks to achieve and the harm (if any) which would be done by the disclosure in question. If the information or document in question were liable to disclose the identity of agents or compromise the security of informers, one would not expect authorisation to be given. If, on the other hand, the document or information revealed matters which, however, scandalous or embarrassing, would not damage any security or intelligence interest or impede the effective discharge by the service of its very important public functions, another decision might be appropriate. Consideration of a request for authorisation

> should never be a routine or mechanical process: it should be undertaken bearing in mind the importance attached to the right of free expression and the need for any restriction to be necessary, responsive to a pressing social need and proportionate.[57]

3.102 Lord Bingham also observed that any decision to refuse authorisation could be judicially reviewed.

3.103 In *Shayler*, Lord Nicholls stated that the fact authorisation can be sought to make a disclosure means that the Official Secrets Act 1989 does not impose a blanket restriction. He observed that a former Crown servant or former member of the security and intelligence services can make a disclosure to a wide range of persons.[58] Indeed, Lord Nicholls observed:

> I do not think that a person who has read the relevant provisions of these statutes and the orders made under them can be said to have been left in any doubt as to wide range of persons to whom an authorised disclosure may be made for the purposes of their respective functions without having first obtained an official authorisation.[59]

3.104 Lord Nicholls concluded that the class of persons from whom official authorisation can be obtained is in fact very wide.[60]

3.105 Crucially, any decision not to grant an individual subject to the Official Secrets Act 1989 official authorisation to disclose information may be judicially reviewed. In *Shayler,* Lord Nicholls observed that "an effective system of judicial review can provide the guarantees that appear lacking in the statute".[61] Lord Hutton elaborated in the following terms:

> I consider that if the appellant were refused official authorisation to disclose information to the public and applied for judicial review of that decision, a judge of the High Court would be able to conduct an inquiry into the refusal in such a way that the hearing would ensure justice to the appellant and uphold his rights under article 6(1) whilst also guarding against the disclosure of information which would be harmful to national security.[62]

3.106 Furthermore, because consideration of this issue involves a right enshrined within the European Convention on Human Rights (specifically Article 10), the decision

[57] *R v Shayler* [2002] UKHL 11; [2003] 1 AC 247 at [30].

[58] Including the Director of Public Prosecutions, the Attorney General and various Cabinet Ministers.

[59] *R v Shayler* [2002] UKHL 11; [2003] 1 AC 247 at [64].

[60] *R v Shayler* [2002] UKHL 11; [2003] 1 AC 247 at [65].

[61] *R v Shayler* [2002] UKHL 11; [2003] 1 AC 247 at [72].

[62] *R v Shayler* [2002] UKHL 11; [2003] 1 AC 247 at [111].

to refuse authorisation would be subject to a more intense standard of review than *Wednesbury* unreasonableness.[63]

3.107 It is important at this stage to point out a distinction in the legislation between former Crown servants and the other categories of individual encompassed by the legislation. Whilst the statute explicitly states that the former can seek authorisation to make a disclosure, the statute does not provide the latter with the same route. Our initial consultation with stakeholders has confirmed, however, that in practice internal procedures do exist to enable such individuals to seek authorisation should they wish to make a disclosure. Even though the fact the process does not exist by virtue of statute, any decision to refuse authorisation would nevertheless be subject to judicial review, as described by Lord Bingham in *Shayler*.

3.108 The House of Lords in *Shayler* assumed that any judicial review would be heard by the High Court, but the Supreme Court has subsequently held that this is not necessarily the case. In *R (on the application of A) v Director of Establishments of the Security Service* the Supreme Court held that by virtue of section 65(2)(a) of the Regulation of Investigatory Powers Act 2000, the Investigatory Powers Tribunal is the only appropriate tribunal in which an action against the security and intelligence services pursuant to section 7 of the Human Rights Act 1998 may be heard.[64]

3.109 Therefore, it may be the case that a failure to grant authorisation to disclose information may be heard by the High Court. It is more likely, however, that it is heard by the Investigatory Powers Tribunal.[65] This is because the appropriate forum will depend upon whether the action is brought against the intelligence services and also upon whether the claimant intends to argue that an action taken by the intelligence services is incompatible with one of the rights enshrined within the European Convention on Human Rights.

3.110 The ability to seek authorisation to make a disclosure is a subject that we will return to in subsequent chapters. The intention here has been simply to set out the process contained within section 7 of the Official Secrets Act 1989.

PROSECUTIONS

3.111 By virtue of section 9(1), no prosecution for an offence under the Official Secrets Act 1989 may be instituted except by or with the consent of the Attorney General, or, as the case may be, the Advocate General for Northern Ireland (i.e. the Attorney General). For the offence in section 4(2), no prosecution may be

[63] If the decision was subject to *Wednesbury* review, it could only be overturned if it was so unreasonable that no reasonable decision maker could have arrived at it. This standard of review is derived from *Associated Provincial Picture Houses Ltd v Wednesbury Corporation* [1948] 1 KB 223; [1947] 2 All ER 680. Given that the decision whether to grant authorisation touches upon a Convention right, a court would invoke the proportionality test. See *Kennedy v Information Commissioner* [2014] UKSC 20; [2015] AC 455. For discussion, see P Craig, *Administrative Law* (8th ed 2016), ch 21.

[64] *R (A) v Director of Establishments of the Security Service* [2009] UKSC 12; [2010] 2 AC 1.

[65] Sections 242 and 243 of the Investigatory Powers Act 2016 amend the relevant provisions in the Regulation of Investigatory Powers Act 2000 that relate to the Investigatory Powers Tribunal. One change will enable decisions of the Investigatory Powers Tribunal to be appealed to the Court of Appeal.

instituted except by, or with the consent of, the Director of Public Prosecutions of England and Wales, or the Director of Public Prosecutions for Northern Ireland.

3.112 In terms of how the Attorney General decides whether to consent to a prosecution, the relevant guidance provides that:

> It is a constitutional principle that when taking a decision whether to consent to a prosecution, the Attorney General acts independently of government applying well established principles of evidential sufficiency and public interest.[66]

3.113 In its report, the Franks Committee examined in detail whether the Attorney General's consent should continue to be required. In doing so, it examined the criticisms made of the Attorney General's role. The Franks Committee explained the Attorney General's function in the following terms:

> The essence of the Attorney General's function under the Official Secrets Acts is that he draws upon his political experience, and is able to obtain the views of the responsible Minister on the national interests, for the purpose of exercising more efficiently his impartial law enforcement role. He is not influenced by party considerations in exercising this role.[67]

3.114 The Franks Committee concluded that the Attorney General's consent function acted to reduce the number of prosecutions brought under the Official Secrets Acts. It also concluded that it was important to retain the Attorney General's role, given the possibility that a disclosure of information protected by the Official Secrets Acts could have implications for international relations.

3.115 The cumulative force of these factors led the Franks Committee to recommend retaining the requirement for the Attorney General to consent before a prosecution could be instituted.

3.116 The requirement that the Attorney General gives consent before a prosecution can be instituted has been a feature of the legislation since the Official Secrets Act 1889. It was assumed in the White Paper that preceded the enactment of the Official Secrets Act 1989 that the Attorney General's consent would continue to be necessary before a prosecution could be instituted. The arguments made by the Franks Committee were not questioned in the White Paper.[68]

3.117 More recently Lord Bingham in *Shayler* stated that:

> The Attorney General will not give his consent to prosecution unless he judges prosecution to be in the public interest. He is unlikely to consent if the disclosure alleged is trivial or the information disclosed stale and notorious or the facts are such as would not be thought by

[66] *Protocol between the Attorney General and the Prosecuting Departments* (2009), para 4(a)2.

[67] Departmental Committee on Section 2 of the Official Secrets Act 1911 (1972) Cmnd 5104, p 95.

[68] Reform of Section 2 of the Official Secrets Act 1911 (1988) Cm 408, para 69.

> reasonable jurors or judges to merit the imposition of criminal sanctions. The consent of the Attorney General is required as a safeguard against ill-judged or ill-founded or improperly motivated or unnecessary prosecutions.[69]

3.118 In *R v Solicitor General, ex parte Taylor* the Divisional Court held that there was no jurisdiction for judicial review of a decision of the Solicitor General to withhold consent to a prosecution under the Contempt of Court Act 1981.[70] So far as we are aware, however, the validity of this case has not been assessed against more recent developments in the law, which might undermine its authority.[71]

SENTENCE

3.119 The overwhelming majority of offences in the Official Secrets Act 1989 are triable either in a magistrates' court or in the Crown Court. For all the offences, except the offences in sections 8(1), 8(4) and 8(5), the maximum sentence if tried in the magistrates' court is a fine and/or six months' imprisonment. If tried in the Crown Court, the maximum sentence is a fine and/or two years' imprisonment.

3.120 The offences in sections 8(1), 8(4) and 8(5) can only be tried in a magistrates' court and carry a maximum sentence of three months' imprisonment and/or a fine.

3.121 The maximum sentence has remained unchanged since the Official Secrets Act 1911 was amended by the Official Secrets Act 1920. The White Paper that preceded the Official Secrets Act 1989 did not consider the appropriateness of this maximum sentence or how it relates to the maximum sentence for other offences of unauthorised disclosure.[72]

3.122 The Franks Committee examined the available penalties in greater detail. The Committee recommended retaining the maximum sentences contained in the Official Secrets Act 1911 on the basis that it received no evidence on their adequacy.[73]

THE DEFENCE OF NECESSITY

3.123 The common law defence of necessity has been raised as a potential defence in two prosecutions under the Official Secrets Act 1989. In *Shayler*, the defendant sought to plead the defence of necessity to an offence under section 1(1) of the Official Secrets Act 1989. In rejecting the application of this defence, the House of Lords expressed regret that the Court of Appeal had engaged with the

[69] *R v Shayler* [2002] UKHL 11; [2003] 1 AC 247 at [35].

[70] *R v Solicitor General, ex parte Taylor* [1996] COD 61. For discussion, see *Consent to Prosecution* (1998) Law Commission Report No 255, para 3.21 – 3.22.

[71] See *R (on the applications of Evans) v Her Majesty's Attorney General* [2015] UKSC 21; [2015] AC 1787, in which Lord Neuberger held that one precept of the rule of law is that the exercise of executive power is subject to review by the courts.

[72] Reform of Section 2 of the Official Secrets Act 1911 (1988) Cm 408, para 67.

[73] Departmental Committee on Section 2 of the Official Secrets Act 1911 (1972) Cmnd 5104, pp 99-100.

argument to the extent that it did on the basis that the defendant "was not within measurable distance" of being able to plead the defence.[74]

3.124 In the case of Katharine Gun, who disclosed information that came into her possession during the course of her work at the Government Communication Headquarters, the defence suggested that Ms Gun also intended to plead necessity as a defence.[75] The Crown Prosecution Service offered no evidence against Ms Gun, which meant that the prosecution was halted before the judge had to evaluate whether to leave the defence to the jury.

3.125 There is disagreement in the case law as to the extent to which there is a general defence of necessity in English and Welsh law. In *R (on the application of Nicklinson) v Ministry of Justice*, for example, the Court of Appeal held that English law knows no general defence of necessity.[76] To the extent that such a defence does exist in English law, necessity has the following elements:

(1) The prohibited act is needed to avoid inevitable and irreparable evil.

(2) No more should be done than is reasonably necessary for the purpose to be achieved.

(3) The evil inflicted must not be disproportionate to the evil avoided.[77]

3.126 Before proceeding in this discussion, it is important to emphasise that necessity as a defence is limited in scope in a number of different ways. First, there is authority to suggest that the defence only applies when there is an element of immediacy.[78] Secondly, the defence can only apply if there exists an identifiable and immediate threat, not one that has passed. Finally, there must be an identifiable adverse consequence that the individual pleading the defence is seeking to avoid.

3.127 Before examining the relationship between the Official Secrets Act 1989 and the defence of necessity, it is important to point out that the courts often conflate this defence with another that exists within the criminal law, namely duress of circumstances. In *Shayler,* Lord Woolf, then the Lord Chief Justice, observed that:

> The distinction between duress of circumstances and necessity has, correctly, been by and large ignored or blurred by the courts.[79]

[74] *R v Shayler* [2002] UKHL 11; [2003] 1 AC 247 at [17].

[75] For discussion, see A Bailin, "The last Cold War statute" (2008) *Criminal Law Review* 625, p 627.

[76] *R (Nicklinson) v Ministry of Justice* [2013] EWCA Civ 961; [2014] 2 All ER 32 at [28].

[77] *Re A (Children: Conjoined Twins: Surgical Separation)* [2000] 4 All ER 961; [2001] 2 WLR 480. For discussion, see D Ormerod and K Laird, *Smith and Hogan's Criminal Law* (14th ed 2015), pp 412-423. A P Simester, J R Spencer, F Stark, G R Sullivan, G J Virgo, *Simester and Sullivan's Criminal Law* (6th ed 2016), pp 821-834.

[78] *R (Nicklinson) v Ministry of Justice* [2012] EWHC 2381 (Admin); [2012] 3 FCR 233 at [74].

[79] *R v Shayler* [2001] EWCA Crim 1977 at [55]

3.128 Despite Lord Woolf's assertion that the courts have been right to ignore the distinction between duress of circumstances and necessity, there are important differences between them, which we list below:

(1) Duress of circumstances cannot be a defence to murder or attempted murder, but there is case law to suggest that necessity may be.

(2) Imminent threats of death or really serious harm are the only occasions for a defence of duress, but not for necessity, so in this respect it is a broader defence.

(3) Necessity is a defence only if the evil the defendant seeks to avoid would be greater than that which they are causing. Duress does not require such a balancing exercise to be undertaken.

(4) The vulnerability of the defendant may be relevant to duress, but not to necessity.

(5) Necessity may create a duty to act, but the same cannot be said of duress.

(6) Duress is generally accepted to be an excuse, whereas necessity is generally seen as being a justification.[80] Duress can be pleaded as a defence under the Official Secrets Act 1989.

3.129 In terms of how any potential defence of necessity and the Official Secrets Act 1989 relate to each other, it is possible for necessity to be pleaded as a defence to an Official Secrets Act offence, subject to two caveats.

3.130 First, as the discussion above demonstrates, the threshold is a very high one. For example, the extent to which it could be said that a damaging disclosure was needed to avoid "inevitable and irreparable evil" could be open to doubt.

3.131 Secondly, the courts may conclude that this common law defence is not available if the offence to which it is pleaded would undermine the "clear legislative policy and scheme" of which the offence forms part.[81] For example in *SC,* the defendant removed her child from the jurisdiction without the permission of the court and was charged with child abduction, contrary to section 1(1) of the Child Abduction Act 1984. The defendant sought to plead necessity, but the Court of Appeal held that the legislative scheme did not permit a defence of necessity. Sir John Thomas, the then President of the Queen's Bench Division, held:

> In the present case, in our view, the legislative policy we have set out is very clear. It is impossible to see how, within the legislative scheme, the legislature could have contemplated that a parent could have the defence of necessity available in respect of the offence of removing a child from England and Wales where the whole purpose of making removal an offence was to reinforce the objective of

[80] For further discussion, see D Ormerod and K Laird, *Smith and Hogan's Criminal Law* (14th ed 2015), p 424. A P Simester, J R Spencer, F Stark, G R Sullivan, G J Virgo, *Simester and Sullivan's Criminal Law* (6th ed 2016), pp 824-831.

[81] *R v Quayle* [2005] EWCA Crim 1415 at [67].

retaining the child within England and Wales so the child could be subject to the protection of the court.[82]

3.132 Given the fact the House of Lords in *Shayler* characterised the Official Secrets Act 1989 as precluding only unauthorised disclosures, it could be argued that to permit an individual to circumvent the routes for making an authorised disclosure by pleading necessity would undermine the statutory scheme. This question, however, has never been decided by the courts.

3.133 In its 2003/2004 Annual Report, the Intelligence and Security Committee of Parliament noted how the courts had developed a defence called "necessity of circumstance".[83] The Committee was not certain that such a defence should exist and what its limit ought to be. As we have discussed in this section, the limits of the defence are clear and it is difficult to envisage circumstances when the defence could be successfully pleaded in the context of the Official Secrets Act 1989.

PROBLEMS WITH THE CURRENT LAW

3.134 Having analysed the current law, this section will examine the extent to which there are any problems with it. Our assessment of the current state of the law is based upon preliminary meetings we have conducted with stakeholders and academic commentary. A list of the individuals, organisations and departments we have met with is contained in Appendix B.

3.135 Our research suggests that the Official Secrets Act 1989 suffers from a number of problems. Some of these problems are attributable to the disparate nature of disclosure offences and the lack of rationality and coherence between them. Other problems are attributable to the manner in which Official Secrets Act 1989 was drafted.

3.136 This section will also ask for consultees' views on a number of ways the current law could be amended so as to rectify these problems.

Requirement to prove damage

3.137 All the offences in the Official Secrets Act 1989, apart from the offences in sections 1(1) and 4(3) require the prosecution to prove that the unauthorised disclosure was damaging to a specified interest or that the information is of such a type that its unauthorised disclosure would be likely to cause such damage.[84]

3.138 As we have discussed, the Government recognised in the White Paper that the requirement to prove damage could hinder the ability to bring prosecutions and enable damaging disclosures of information to be made with impunity. The Government expressed the view that it would be deeply undesirable for those

[82] *R v SC* [2012] EWCA Crim 389 at [13].

[83] Intelligence and Security Committee, Annual Report 2003-2004 (June 2004) Cm 6240, p 42. The Committee as currently constituted has expressed no view on the Official Secrets Acts 1911-1989.

who disclosed information which caused damage to "be able to do so with impunity, simply by reason of the sensitivity of the subject matter".[85]

3.139 Proof that damage was caused will involve the prosecution having to confirm the harm to the specified interest – national security, international relations etc – which the defendant's unauthorised disclosure caused. The public confirmation that such damage has occurred has the potential to compound the damage caused by the initial unauthorised disclosure. In some cases it may be that the state would rather not confirm or compound the damage, but that will mean that the discloser of the information cannot be prosecuted despite the clear wrongdoing involved. With the aim of avoiding this situation, the legislation provides that the damage requirement can be satisfied if the prosecution proves that a particular disclosure was of a certain class or description, and that disclosure of information of that class or description was likely to cause the requisite damage.[86]

3.140 It is necessary to evaluate the extent to which the legislation achieves the aim of ensuring that individuals are not free to make damaging disclosures with impunity simply by reason of the sensitivity of the subject matter disclosed. It would be undesirable if those who disclose the most sensitive information were rendered immune from prosecution. Indeed, it has been argued that:

> The extraordinary Catch-22 is that the greater the sensitivity and intrinsic important to national security of the information compromised in the media, the greater the incentive for governmental inaction [i.e. no prosecution].[87]

3.141 A similar point was made by Lord Nicholls in *Shayler*:

> Damage already done may well be irreparable, and the gathering together and disclosure of evidence to prove the nature and extent of the damage may compound its effects to the further detriment of national security.[88]

3.142 It is important to note that some procedural measures exist to limit the prospect of this problem occurring. Section 8(4) of the Official Secrets Act 1920 provides that the public, or a portion of the public, can be excluded from a hearing if publication of any evidence to be given or of any statement to be made in the course of the proceedings would be prejudicial to the national safety.

3.143 Despite the existence of this provision, preliminary consultation with stakeholders has suggested that the damage element of the offences can pose an insuperable hurdle to bringing a prosecution. This impediment is not only caused by the inherent sensitivity of the information the defendant disclosed, but due to the

[85] Reform of Section 2 of the Official Secrets Act 1911 (1988) Cm 408, para 39.

[86] Although it is unclear how this would be interpreted, it has been suggested that proof of the objective risk of damage is insufficient to constitute the offence. See D Ormerod and D Perry (eds), *Blackstone's Criminal Practice* (2017), at B9.45.

[87] Foreign Denial and Deception Committee, *Leaks: How Unauthorized Media Disclosures of US Classified Intelligence Damage Sources and Methods* (24 April 2002), p 4.

[88] *R v Shayler* [2002] UKHL 11; [2003] 1 AC 247 at [85].

requirement to prove either that the disclosure of that information caused damage to a specified interest, or that it was of a type of information that was likely to do so. It is this requirement to prove the existence of a vulnerability that poses the obstacle. As Lord Nicholls explained in *Shayler,* "disclosure of evidence to prove the nature and extent of the damage may compound its effects to the further detriment of national security." Therefore although all the elements of a criminal offence may be present, proving them to the requisite criminal standard risks compounding the damage caused by the initial disclosure. We recognise that our research stands in contrast to those commentators who expressed the view that the damage requirement would be easy to satisfy.[89] Practical experience has demonstrated, however, that this is not the case.

3.144 As our discussion of the other offences that criminalise the unauthorised disclosure of information demonstrates, most offences do not require proof that the disclosure was damaging.[90] This includes offences that criminalise the disclosure of information relating to national security and which carry a higher maximum sentence than the offences contained in the Official Secrets Act 1989. The Official Secrets Act 1989 is not representative of how such disclosure offences are typically drafted. One explanation for this is the fact that the damage requirement was included in the Official Secrets Act 1989 because the Government rejected the earlier proposal to rely upon a ministerial certificate to prove the essential elements of the offence.

3.145 As we have explained, the Government foresaw that the requirement to prove actual damage could pose an insuperable barrier to prosecuting those who commit disclosures without lawful authority. To avoid this, it therefore suffices if the disclosure was of a certain class or description, and disclosure of information of that class or description was likely to cause the requisite damage. None of these terms are defined.

3.146 Although the legislation absolves the prosecution of the burden of proving that the disclosure in fact caused damage, the prosecution must still prove that the information in question fell within a certain class or description and that the disclosure of information within that class or description was likely to cause the requisite damage. Our initial consultation with stakeholders suggests that the requirement to prove that the disclosure of such a category of information *was likely to cause* the requisite damage can *still* pose an insurmountable barrier to initiating a prosecution.

3.147 We believe it is undesirable in principle for those who have committed unauthorised disclosures of the types specified in the legislation to be able to avoid liability on the basis that a prosecution for that wrongdoing would potentially cause further damage.

Provisional conclusion 9

3.148 **We provisionally conclude that, as a matter of principle, it is undesirable for those who have disclosed information contrary to the Official Secrets Act 1989 to be able to avoid criminal liability due to the fact that proving the**

[89] For example, see G Robertson, *Freedom, the Individual and the Law* (1993), p 167.

[90] See the discussion in Chapter 4 for analysis.

damage caused by the disclosure would risk causing further damage. Do consultees agree?

The structure and nature of the offences

3.149 Related to the problem identified above is the fact that the way the offences are drafted no longer relates to how they are applied in practice. On their face, the offences contained in the Official Secrets Act 1989 are offences of strict liability, as there is no need to prove, for example, that the defendant intended to cause damage to the capability of the armed forces of the Crown in order for him or her to be guilty of an offence contrary to section 2. As we have discussed above, however, as a result of the judgment of the Court of Appeal in *Keogh* it is not accurate to describe the offences as being offences of strict liability. The Court of Appeal did state, however, that an individual could still be guilty of an offence without inviting the jury to engage in a subjective assessment of the defendant's state of mind.

3.150 It could be argued that this discrepancy between the drafting of the offences and how they are understood in practice is problematic. If the offences were drafted so as to make the requirement to prove fault explicit, then it would be possible to have graduated offences that better reflected the defendant's culpability.

Provisional conclusion 10

3.151 **We provisionally conclude that proof of the defendant's mental fault should be an explicit element of the offence contained in the Official Secrets Act 1989. Do consultees agree?**

3.152 Assuming that consultees agree with our previous provisional conclusions, we will now examine how the offences could be restructured.

3.153 As we have already discussed, most of the criminal offences currently contained in the Official Secrets Act 1989 require proof that the defendant's unauthorised disclosure caused, or was likely to cause, a prohibited result.

3.154 One option that we believe would remedy the difficulty of being unable to prove that the disclosure caused or was likely to cause the requisite damage is to shift the offences so that they focus on the defendant's conduct and their culpability for engaging in that conduct. Such offences are often described as being drafted in the "inchoate mode". This term has been defined in the following way:

> The inchoate mode is characterised by a style of defining criminal offences which proscribes the doing of certain acts in order to produce a certain outcome. It is the outcome which the law wishes to prevent, but the offence is so defined as to penalise the defendant for trying to produce it, whether or not the outcome resulted.[91]

3.155 There are numerous examples of such offences throughout the criminal law. The offence of burglary, contained in section 9(1)(a) of the Theft Act 1968 is an example that has been given by Ashworth. A person commits burglary if they

[91] A Ashworth, "Defining criminal offences without harm" in P Smith (ed), *Criminal Law: Essays in Honour of JC Smith* (1987), p 8.

enter a building as a trespasser with the intention of committing either theft, grievous bodily harm, or criminal damage.

3.156 As Ashworth explains, one reason why an offence might be drafted in the inchoate mode is to reduce problems of proof.[92] In the present context, we are suggesting that there would be benefits if the offences as they are currently drafted in the Official Secrets Act 1989 were recast so that they focused on the defendant's conduct. There is precedent for such an approach in a different context. The Fraud Act 2006 criminalises fraudulent conduct, irrespective of whether it succeeds in deceiving anyone and irrespective of whether it led to the defendant obtaining any property.[93] The Act was drafted in this way to overcome two problems that undermined the effectiveness of the previous law. First, it was difficult under the old law to prove that someone was deceived. Secondly, it was difficult to prove that the deception caused the defendant to obtain the property in question.[94] These difficulties were overcome by drafting the offences so that they were non-result based.

3.157 Aside from these practical issues, as a matter of principle, it could also be argued that it is undesirable for criminal liability to depend upon whether the disclosure in question resulted or was likely to result in the requisite harm. This is because whether the harm results or was likely to result is largely beyond the defendant's control; it could therefore be a matter of mere luck.[95]

3.158 One way of addressing the issue that stakeholders have brought to our attention is for an offence to be committed if a member of the security and intelligence agencies, notified person, Crown servant or government contractor discloses information that falls within the scope of the Official Secrets Act 1989 irrespective of whether the disclosure caused, or was likely to cause damage to a specified interest.

3.159 We are keen to ensure that the threshold of culpability that must be crossed before an individual commits a criminal offence for disclosing information without lawful authority is not lowered. One way we believe this aim could be achieved is to redraft the offences so that they explicitly incorporate a greater fault element. As our analysis of the current law explained, despite the fact the Court of Appeal in *Keogh* held that the defendant must know or have reasonable grounds to believe that the information fell within one of the categories encompassed by the Official Secrets Act 1989 and that its disclosure would or would be likely to cause the requisite damage, the court nevertheless concluded that an individual could be guilty without inviting the jury to engage in a subjective assessment of the

[92] A Ashworth, "Defining criminal offences without harm" in P Smith (ed), *Criminal Law: Essays in Honour of JC Smith* (1987), p 17.

[93] For example, the offence of fraud by false representation under section 2(1) of the Fraud Act 2006 is committed when a person dishonestly makes a false representation and intends either to make a gain or cause loss to another, regardless of whether the gain or loss did in fact occur.

[94] See J Horder, *Ashworth's Principles of Criminal Law* (8th ed 2016) pp 417-418. For detailed discussion of the problems, see *Fraud* (2002) Law Commission Consultation Paper No 276, pp 15-23.

[95] For discussion, see J C Smith, "The Element of Chance in Criminal Liability" (1971) *Criminal Law Review* 63.

defendant's state of mind. The court assumed, therefore, that the term 'reasonable grounds to believe' imports an objective evaluation.

3.160 Unlike the Court of Appeal in *Keogh*, we believe the fault element ought to be subjective. This would compensate for the fact the defendant's unauthorised disclosure no longer has to cause, or be likely to cause, the requisite damage.

3.161 Below we have set out an example of how we believe the offences could be redrafted. This model shifts the focus of the offence from being on the result of the defendant's unauthorised disclosure, to their culpability, as reflected by their state of mind when the information in question was disclosed without lawful authority:

(1) A person commits an offence if he or she intentionally makes an unauthorised disclosure of information relating to security and intelligence, defence or international relations knowing that that disclosure is capable of damaging security and intelligence, defence or international relations.

(2) A person commits an offence if he or she intentionally makes an unauthorised disclosure of information relating to security and intelligence, defence or international relations having reasonable grounds to believe that that disclosure is capable of damaging security and intelligence, defence or international relations.

3.162 The term "damage" would have the meaning it currently has in the legislation. In the context of information relating to defence, for example, the prosecution would need to prove that the defendant, in making the disclosure without lawful authority, knew that the disclosure of the information was capable of damaging the capability of the armed forces of the Crown, or had reasonable grounds for believing that it was capable of doing so.

3.163 This model has the benefit of ensuring that the offences explicitly incorporate a fault element. In addition, this model would not dilute the culpability that must be present before an individual is guilty of a criminal offence for disclosing information that falls within a protected category without authorisation.

Consultation question 6

3.164 **We welcome consultees' views on the suitability of shifting to non-result based offences to replace those offences in the Official Secrets Act 1989 that require proof or likelihood of damage.**

3.165 The question of how best to restructure the offences is made more complex by the fact that the elements of the offences differ when it comes to members of the security and intelligence agencies and notified persons. We have provisionally concluded that there is still force in the reasons relied upon in the White Paper to justify treating these categories as different from others. Principally that membership of the security and intelligence services carries with it a special and inescapable duty of secrecy and such disclosures may reduce public confidence in the services' ability to carry out their duties effectively and loyally.

3.166 One way to ensure that this difference continues to be reflected is for the offences to continue to be offences of strict liability in the context of members of the security and intelligence services and notified persons.

Provisional conclusion 11

3.167 **With respect to members of the security and intelligence agencies and notified persons, the offences should continue to be offences of strict liability. Do consultees agree?**

Delineating who is subject to the provisions in the Official Secrets Act 1989

3.168 The Official Secrets Act 1989 applies to:

(1) Members and former members of the security and intelligence services.

(2) Persons notified they are subject to the provisions of the Act.

(3) Crown servants and former Crown servants.

(4) Government contractors.

3.169 Stakeholders have suggested that there are numerous problems with the way in which the legislation brings certain officeholders within its remit. First, the meaning of the term "member of the security and intelligence services" is obscure. For example it is unclear whether the term "member" is intended to be synonymous with employee or whether it is intended to be broader.

3.170 Secondly, there is a more fundamental problem with the concept of a "notified person". By virtue of section 1(6), notification that a person is subject to the Act has effect by way of a notice in writing served on them by a Minister of the Crown. Such a notice will be served if, in the Minister's opinion, "the work undertaken by the person in question is or includes work connected with the security and intelligence services and its nature is such that the interests of national security require that he should be subject to the provisions of that subsection".[96]

3.171 If an individual has been notified that they are subject to the Act, then they commit an offence contrary to section 1(1) of the Official Secrets Act 1989 if they disclose information without authorisation, without the need for the prosecution to prove that the disclosure was damaging. A notified person is therefore treated in the same way in the legislation as a member of the security and intelligence services.

3.172 Notification can fulfil two potential functions. First it makes an individual subject to the provisions of the Official Secrets Act 1989 when they would not otherwise be subject to the legislation, for example because they are not a Crown servant. Secondly, even if an individual would be subject to the provisions of the

[96] By virtue of section 1(7) a notification remains in force for five years beginning on the day on which it is served and may be renewed by further notices for periods of five years at a time. Section 1(8) provides that a notification may be revoked by a further notice in writing by the Minister to the person concerned as soon as, in the Minister's opinion, the worked undertaken by that person ceases to fall within section 1(6).

legislation, for example because they are a Crown servant, it aligns that person with members of the security and intelligence services for the purpose of the offence contained in section 1(1) of the Official Secrets Act 1989.

3.173 Currently the legislation requires a department to compile a list of posts that, because of the nature of the work undertaken by people in those posts, the staff who occupy them ought to be notified. Once a list of the individuals in those posts has been compiled, it must then be submitted to the Secretary of State. After it has been approved, the notification only takes effect once it has been served on the individual in question. Although this procedure sounds unproblematic in theory, our initial consultation with stakeholders suggests that in practice the statutory procedure for notification is overly bureaucratic, which impedes its effectiveness and may mean a person is not notified when they ought to be. This has the potential to cause gaps in the protection the Official Secrets Act 1989 is intended to afford to information.

3.174 This is attributable to two factors. First, the process is slow and does not reflect the fact that sometimes a person must be notified at short notice. Secondly, it assumes that the list of those who ought to be notified remains largely static. In practice, however, this is not the case, given the internal restructuring that can take place within a department.

3.175 The experience of using the notification process since the Official Secrets Act 1989 suggests that it does not work as well as it should.

3.176 The final issue relates to the definition of Crown servant. The definition of Crown servant is contained in section 12 of the Official Secrets Act 1989. By virtue of sections 12(1)(f) and 12(1)(g), the Secretary of State can include within the definition of Crown servant members or employees of a prescribed body and any person who is the holder of a prescribed office or who is an employee of such a holder. Initial consultation with stakeholders suggests that this process is bureaucratic and cumbersome and in need of improvement.

3.177 One issue is that when setting up a body, such as the Civil Aviation Authority, it is not possible to specify in the legislation setting up the organisation in question that its employees are deemed to be Crown servants for the purpose of section 12 of the Official Secrets Act 1989. This can only be achieved by invoking the mechanism contained in sections 12(1)(f) and 12(1)(g) of the Official Secrets Act 1989. It could be less time consuming if this aim could also be achieved through primary legislation, which would supplement the current mechanism.

Provisional conclusion 12

3.178 **The process for making individuals subject to the Official Secrets Act 1989 is in need of reform to improve efficiency. Do consultees agree?**

Consultation question 7

3.179 **If consultees agree with provisional conclusion 12, do consultees have a view on whether these options would improve the efficiency of the process for making individuals subject to the Official Secrets Act 1989?**

(1) Member of the security and intelligence services – As we have discussed, it is not entirely clear what is intended to be meant by the term "member". One option is to amend the term to clarify that employees, seconded and attached staff, in addition to those working under a contract of service, fall within the scope of the offence in section 1(1).

(2) Notified person – We have provisionally concluded that notification does serve a useful function and ought to be retained. We do believe, however, that there are two ways the process could be improved. First, new guidance could be issued clarifying when an individual ought to be subject to notification. Secondly, the length of time a notification is in force could be lengthened. It is possible, however, to envisage more fundamental reform that would further reduce the administrative burden. One option is to specify the types of post that ought to be subject to notification. Rather than focusing upon the individual, the focus would be on the post. A second option would be to replace the notification provisions and expand the scope of section 1(1) to anyone who has, or has had access to security and intelligence information by virtue of their office or employment or contract of services.

(3) Definition of Crown servant – We provisionally conclude that the process for expanding the definition of Crown servant ought to be streamlined and that it should be possible to make an officeholder a Crown servant for the purposes of the Official Secrets Act 1989 by way of primary legislation, in addition to the process set out in section 12 of the Act.

Sentence

3.180 The majority of the offences in the Official Secrets Act 1989 are triable either in a magistrates' court or in the Crown Court. The maximum sentence for the majority of the offences is six months' imprisonment and/or a fine if tried in a magistrates' court and two years' imprisonment and/or a fine if tried in the Crown Court. The offence in sections 8(1), 8(4) and 8(5) is triable only in a magistrates' court and carries a maximum sentence of three months' imprisonment.

3.181 As we explained above, the unauthorised disclosure offences in the Official Secrets Acts have carried a maximum sentence of two years' imprisonment for many years. In the White Paper that preceded the 1989 Act, the Government did not engage substantively with whether these sentences are appropriate. In addition the Franks Committee, when it conducted its review of section 2 of the Official Secrets Act 1911, did not receive any evidence on the whether the two year maximum sentence was appropriate.

3.182 More recently, however, the Intelligence and Security Committee of Parliament has commented that:

> There are startlingly inconsistent sentences for broadly similar offences, while the existing legislation fails to distinguish between offences which vary considerably in the seriousness of their consequences. Offences under the 1911 Act carry a penalty of up to

> 14 years' imprisonment. Offences under the 1989 Act carry sentences no higher than two years' imprisonment.
>
> Disclosing the names of agents, and thus endangering their lives, may require a substantially higher penalty than is currently available under the 1989 Act. Consideration should therefore be given to the introduction of a more gradual series of penalties.[97]

3.183 As we discuss in Chapter 4, our research has demonstrated the existence of numerous offences that criminalise the unauthorised disclosure of various categories of information. The vast majority of these offences carry maximum sentences of two years' imprisonment if tried in a Crown Court. There are others, however, that carry a higher maximum sentence.

3.184 The maximum sentence for the offences contained in the Official Secrets Act 1989 is the same as many other offences that criminalise the unauthorised disclosure of information. For example, it is an offence punishable by up to two years' imprisonment for an employee of the National Lottery Commission to disclose information that has been supplied by Her Majesty's Commissioners for Revenue and Customs that relates to a person whose identity is specified in the information or whose identity can be deduced from the information. This is the same maximum sentence available for an unauthorised disclosure that, to take one example, damages the capability of the armed forces to carry out their tasks.

3.185 By way of contrast, sections 57 – 59 of the Investigatory Powers Act 2016, when commenced, will make it an offence punishable by up to five years' imprisonment for a Crown servant to disclose without authorisation anything to do with the existence or implementation of particular warrants granted pursuant to the Investigatory Powers Act, including the content of intercepted material and related communications data. Appendix C sets out a list of other disclosure offences that our research has brought to light.

3.186 When compared with these wider disclosure offences, it could be argued that the maximum sentence available for the offences in the Official Secrets Act 1989 does not adequately reflect the culpability in the most egregious cases involving unauthorised disclosure of information that causes damage to the interests listed in the 1989 Act.

3.187 Additionally, the maximum sentence for the offences in the Official Secrets Act 1989 is low when compared with offences that exist in other jurisdictions that criminalise similar forms of wrongdoing, as suggested by our comparative law research in Appendix A. For example, the maximum sentence for making an unauthorised disclosure in Canadian law under the Security of Information Act 2001 is 14 years' imprisonment.[98]

3.188 In the digital age, the volume of information that can be disclosed without authorisation is much greater than when the Official Secrets Act 1989 was

[97] Intelligence and Security Committee, 2003-2004 Annual Report (June 2004) Cm 6240, p 43. The Committee as currently constituted has expressed no view on the Official Secrets Acts 1911-1989.

[98] Security of Information Act 2001, s 14(2).

originally drafted. It could be argued that this means that the ability to cause damage to the national interest and the risk of such damage occurring has also increased. It could be argued that there is also a corresponding increase in culpability in such cases.

Provisional conclusion 13

3.189 **We provisionally conclude that the maximum sentences currently available for the offences contained in the Official Secrets Act 1989 are not capable of reflecting the potential harm and culpability that may arise in a serious case. Do consultees agree?**

Receiving legal advice

3.190 It has been argued that the Official Secrets Act 1989 has the potential to interfere with a defendant's unfettered right to instruct his legal advisors.[99] This is attributable to the fact the term "disclose" is not defined as "to make public", but includes "parting with possession of". The consequence of this, it is argued, is that a suspect or person charged with an offence contrary to the Official Secrets Act 1989 might potentially commit further offences when instructing their legal advisors. In instructing their legal advisors, the defendant, a former member of the security and intelligence services for example, might disclose information that relates to security or intelligence. Unless the defendant sought authorisation before making those disclosures, they would commit an offence under section 1(1) of the Official Secrets Act 1989.

3.191 In *Shayler,* Lord Bingham accepted that the fair hearing guarantee in Article 6(1) of the European Convention on Human Rights must ordinarily carry with it the right to seek legal advice and assistance from a lawyer outside government service. He observed that this was a matter to be resolved by seeking authorisation under section 7(3)(b) of the Official Secrets Act 1989 and could not foresee circumstances in which it would be proper for the service to refuse its authorisation for any disclosure at all to a qualified lawyer from whom the former member wished to seek advice. Lord Bingham stated that the service would be entitled to limit its authorisation to material in a redacted or anonymised form. He suggested that a special advocate could be instructed to represent the former member's interests if the material in question was too sensitive to be disclosed to their nominated lawyer.[100]

3.192 It is important to point out that Lord Bingham was considering this issue in the context of a member or former member of the security and intelligence services seeking judicial review of a denial by the service to authorise a disclosure. He was not considering this issue in the context of a member or former member seeking to instruct a lawyer in criminal proceedings for the unauthorised disclosure of information. Arguably the problem is more acute in the context of criminal proceedings.

3.193 As Lord Bingham suggested, a member or former member of the security and intelligence services facing criminal prosecution could avoid liability by seeking

[99] A Bailin, "The last Cold War statute" (2008) *Criminal Law Review* 625, p 629.

[100] *R v Shayler* [2002] UKHL 11; [2003] 1 AC 247 at [34].

authorisation to make the disclosure in question. It could, however, be considered contrary to principle to require the defendant to seek authorisation before they can instruct their legal advisors without risking the commission of a further criminal offence.

3.194 We believe that there are ways this issue could be rectified. The issue of potentially committing further criminal offences when instructing legal advisors has arisen recently in the context of the Investigatory Powers Act 2016. There are sections in the Investigatory Powers Act 2016 that, when commenced, will impose a duty not to make unauthorised disclosures. Failure to comply with this duty is a criminal offence. Certain disclosures, however, are categorised as exempt disclosures. One category of exempt disclosure relates to a disclosure that is made to a professional legal adviser by their client for the purpose of receiving legal advice. This does not apply if the disclosure is made with a view to furthering any criminal purpose.[101]

3.195 The purpose of setting out the relevant clauses from the Investigatory Powers Act 2016 is to demonstrate that there are ways of overcoming the problem that has been identified within the Official Secrets Act 1989. We believe that a similar approach could be taken in the present context. We believe, however, that an exemption for disclosure to a legal advisor should be restricted to a legal advisor who is a barrister, solicitor or legal executive, with a current practising certificate. As Lord Bingham suggested in *Shayler* we would expect this legal advisor to comply with any obligations that may be imposed upon them that relate to the need to safeguard information relating to the case.

3.196 To avoid a gap in the protection the legislation is intended to afford sensitive information, we would expect a disclosure only to constitute an "exempt disclosure" if it was made to a qualified solicitor, barrister or legal executive with a current practising certificate, it was made for the purpose of receiving legal advice in relation to proceedings for an offence contrary to the Official Secrets Act 1989, it was not made with the intention of furthering a criminal purpose and it complied with any vetting and security requirements as might be specified

Provisional conclusion 14

3.197 **A disclosure made to a professional legal advisor who is a barrister, solicitor or legal executive with a current practising certificate for the purposes of receiving legal advice in respect of an offence contrary to the Official Secrets Act 1989 should be an exempt disclosure subject to compliance with any vetting and security requirements as might be specified. Do consultees agree?**

Prior publication

3.198 It has been suggested that it is problematic for the Official Secrets Act 1989 to contain no defence of prior publication.[102] Although prior publication might be relevant to the question of whether the disclosure in question was damaging, this does not “prevent a prosecution under the 1989 Act for disclosure of something

[101] See sections 57 to 59 of the Investigatory Powers Act 2016.

[102] A Bailin, “The last Cold War statute” (2008) *Criminal Law Review* 625, p 629.

which is already largely in the public domain".[103] This stands in contrast to the Government's 1979 Bill, in which it would not have been an offence to disclose without lawful authority information in certain categories if the defendant could show that the information had been made available to the public before this disclosure. The rationale for this was the assumption that if the information was already in the public domain, a second disclosure could not be harmful.

3.199 The Government considered this issue in the White Paper. The following viewpoint was expressed:

> It seems to the Government that this rationale is flawed. There are circumstances in which the disclosure of information in any of the categories which the Government proposes to cover in new legislation may be harmful even though it has previously been disclosed. Indeed, in certain circumstances a second or subsequent disclosure 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. But confirmation of that story by, say, a senior official of the relevant Government Department would be very much more damaging.[104]

3.200 Although this example has been described as "chilling", we believe there is validity in the argument made in the White Paper.[105] For example, a website could publish a list of names of individuals it asserts colluded with the authorities in Northern Ireland. If an individual within Government confirmed the validity of these names, it could magnify the damage caused by the initial disclosure.

3.201 One option to deal with this possibility is for a defence to be available only if the defendant proves that the information was already lawfully in the public domain as a matter of fact, for example because it was disclosed as a result of a request made under the Freedom of Information Act 2000 and no exemption was invoked to justify not disclosing the information.

3.202 There is a challenge, however, as to what is meant by "in the public domain". Birkinshaw and Varney, commenting on the history of the defence of prior publication in relation to the Protection of Information Bill 1979, have noted that:

> In the Lords an amendment was moved allowing a defence where "before the time of the alleged offence the information in question had become *widely disseminated* to the public whether in the UK or elsewhere" adding "there was no reasonable likelihood that its further disclosure would damage the work of, or any part of, the security and intelligence services". This latter part was to meet the government's objection to such a defence, viz additional or more serious damage

[103] A Bailin, "The last Cold War statute" (2008) *Criminal Law Review* 625, p 629.

[104] Reform of Section 2 of the Official Secrets Act 1911 (1988) Cm 408, paras 62-64.

[105] A Bailin, "The last Cold War statute" (2008) *Criminal Law Review* 625, p 629.

would be perpetrated by a second or further disclosure.[106] (Emphasis added)

3.203 We believe that the defence of prior publication ought only to operate if the defendant proves that the information has become widely disseminated to the public.

Provisional conclusion 15

3.204 **We provisionally conclude that a defence of prior publication should be available only if the defendant proves that the information in question was in fact already lawfully in the public domain and widely disseminated to the public. Do consultees agree?**

The categories of information protected by the legislation

3.205 It has been argued that the categories of information protected by the Official Secrets Act 1989 raise difficult issues of interpretation[107] and are too wide.[108] As we have already discussed, the aim of the Government in repealing section 2 of the Official Secrets Act 1911 and replacing it with the Official Secrets Act 1989 was to narrow the categories of information which could trigger a criminal sanction.

3.206 The Government sought to identify those categories of information which, if disclosed, would be sufficiently harmful to the public interest to justify the application of criminal sanctions. We set these out in our analysis of the current law.

3.207 Some of the categories of information are defined with greater precision than others. For example, the category protected by section 3 of the Official Secrets Act 1989, international relations, has been singled out as being "troublingly wide".[109]

3.208 We have received no evidence, however, to substantiate the view that the categories of information encompassed by the Official Secrets Act 1989 are too broad. Bearing in mind the necessity of ensuring that sensitive information does not lose the protection of the criminal law, we would welcome consultees' views on whether the categories should be narrowed and, if so, how.

Consultation question 8

3.209 **We would welcome consultees' views on whether the categories of information encompassed by the Official Secrets Act 1989 ought to be more narrowly drawn and, if so, how.**

[106] P Birkinshaw and M Varney, *Government and Information: The Law Relating to Access, Disclosure and their Regulation* (4th ed 2011), p 235.

[107] A Bailin, "The last Cold War statute" (2008) *Criminal Law Review* 625, p 629.

[108] G Robertson, *Freedom, the Individual and the Law* (1993), pp 168-173.

[109] For discussion, see G Robertson, *Freedom, the Individual and the Law* (1993), p 170.

3.210 One specific issue that has been brought to our attention however, and that we believe merits further consideration, is the fact that sensitive economic information is currently not protected by the Official Secrets Act 1989. This is an issue that was considered by the Franks Committee. Although the Franks Committee concluded that the possibility of some harm to the economy was not a sufficiently sound criterion to justify criminalisation, it also concluded that:

> Exceptionally grave injury to the economy qualifies for the protection of criminal sanctions… It is not simply a question of a drop in the standard of living; such injury could have wider repercussions on the life of the nation.[110]

3.211 The Franks Committee concluded that information relating to the currency and that could impact negatively upon the exchange rate, ought to be protected by the criminal law from unauthorised disclosure.[111]

3.212 Whilst being mindful of the need to ensure that the legislation only encompasses information the disclosure of which could damage the national interest, we invite consultees' views on whether information that relates to the economy ought to be brought within the scope of the legislation.

3.213 One way to define this category is to specify that it only encompasses information that affects the economic well-being of the United Kingdom in so far as it relates to national security. This formulation is utilised in the Investigatory Powers Act 2016, which was recently approved by Parliament. This term is used in the context of the grounds upon which the Secretary of State may issue a targeted interception warrant or a targeted examination warrant. Given the context in which this term is used, it is not surprising that it is narrowly defined. Consultees may take the view, however, that a broader definition is desirable to maximise legislative protection. It is for that reason that we are seeking consultees' views on the suitability of this term in the context of criminal offences intended to safeguard official information.

Consultation question 9

3.214 **Should sensitive information relating to the economy in so far as it relates to national security be brought within the scope of the legislation or is such a formulation too narrow?**

The territorial ambit of the offences

3.215 As we discussed in the previous chapter, the criminal law is territorial, which means that "misconduct committed outside the realm cannot ordinarily amount to the conduct element of an offence under English law".[112] The courts in England and Wales have typically adopted a terminatory approach to jurisdiction. This

[110] *Departmental Committee on Section 2 of the Official Secrets Act 1911* (1972) Cmnd 5104, pp 51-52.

[111] For an analysis of the extent to which section 1 of the Official Secrets Act 1911 encompasses economic information, see R Thomas, *Espionage and Secrecy* (1991), pp 48-50.

[112] M Hirst, *Jurisdiction and the Ambit of the Criminal Law* (2003), p 3. See also G Williams, "Venue and the Ambit of the Criminal Law (Part 3)" (1965) 81 *Law Quarterly Review* 518.

means that the courts will accept jurisdiction to try an offence when the "last act" was performed in this jurisdiction or, if the offence is a result crime, when the prohibited result occurred in this jurisdiction. In some cases, however, the courts have taken a more flexible approach. In *Smith (No 4),* the Court of Appeal preferred, on policy grounds, to apply a more flexible test, giving the English courts a broader jurisdiction over conduct where "a substantial measure of the activities constituting the crime take place in England".[113] The validity of this approach was confirmed by the Court of Appeal more recently in *Rogers* and *Sheppard*.[114]

3.216 As we discussed above, the Official Secrets Act 1989 represents an exception to the rule that the criminal law is territorial. This is because an individual who is a British citizen or Crown servant can commit an offence contrary to the Official Secrets Act 1989 even if they are outside the United Kingdom when the information in question was disclosed without authorisation.[115] This does not apply to those offences that can only be tried in the magistrates' court, which are contained in section 8(1), 8(4) and 8(5) of the Official Secrets Act 1989. Hirst has argued that, "the nature and quality of the offences concerned [i.e. those contained in the Official Secrets Acts] demand some kind of extraterritorial ambit in order to be effective."[116] The issue that we are considering in this section is whether the extraterritorial ambit of the offences is sufficient to ensure they remain effective.

3.217 As we discussed earlier, a person who is not a British citizen or Crown servant does not commit an offence if they disclose the information outside the United Kingdom. This is true even if they are a "notified person", as defined in section 1 of the Official Secrets Act 1989. We believe it is necessary to consider the extent to which this creates a gap in the protection the legislation affords sensitive information.

3.218 For example, an individual may be a non-British citizen seconded to a government department and in that role have access to information that relates to security and intelligence. Such an individual may be a notified person for the purposes of section 1 of the Official Secrets Act 1989. If that person were to retain the information and disclose it upon their return to their home country, however, they would not commit an offence contrary to the law of England and Wales.

3.219 Such a scenario could perhaps not have been envisaged when the Official Secrets Act 1989 was drafted, given the inability to store and transfer large quantities of information with relative ease. That perhaps explains why the legislation does not extend to unauthorised disclosures perpetrated by non-British notified persons abroad.

[113] *R v Smith (No 4)* [2004] EWCA Crim 631; [2004] 3 WLR 229 at [55].

[114] *R v Rogers* [2014] EWCA Crim 1680; [2015] 1 WLR 1017 at [54]; *R v Sheppard* [2010] EWCA Crim 65; [2010] 1 WLR 2779.

[115] M Hirst, *Jurisdiction and the Ambit of the Criminal Law* (2003), pp 223-224.

[116] M Hirst, *Jurisdiction and the Ambit of the Criminal Law* (2003), p 224.

3.220 The challenges the digital age poses to orthodox notions of territoriality has been the subject of academic interest.[117] Domestically, it has led to recent changes being made to the Computer Misuse Act 1990 by the Serious Crime Act 2015.

3.221 Under that legislation as amended, a defendant can be convicted before an English court if they were a British citizen at the time they are alleged to have committed the offence. An individual can commit an offence contrary to the Computer Misuse Act 1990 even if they were outside the United Kingdom when they are alleged to have committed the offence provided there is a "significant link" with the United Kingdom. The Act defines "significant link" in a number of different ways.[118]

3.222 There are a number of other provisions that take a novel approach to the territorial ambit of the criminal law. For example, section 11(2) of the European Communities Act 1972 creates an offence that applies to members of the European Atomic Energy Community institutions or committees.[119] The offence is defined as follows:

> (2) Where a person (whether a British subject or not) owing either—
>
> (a) to his duties as a member of any Euratom institution or committee, or as an officer or servant of Euratom; or
>
> (b) to his dealings in any capacity (official or unofficial) with any Euratom institution or installation or with any Euratom joint enterprise;
>
> has occasion to acquire, or obtain cognisance of, any classified information, he shall be guilty of a misdemeanour if, knowing or having reason to be believe that it is classified information, he communicates it to any unauthorised person or makes any public disclosure of it, whether in the United Kingdom or elsewhere and whether before or after the termination of those duties or dealings; and for this purpose "classified information" means any facts, information, knowledge, documents or objects that are subject to the security rules of a member State or of any Euratom institution.

3.223 The ambit of this offence is sufficiently broad to encompass conduct by a non-British citizen outside the United Kingdom. The offence therefore follows the information, which does not lose its protection simply because the defendant was abroad when they made the unauthorised disclosure. This offence therefore demonstrates that different approaches to jurisdiction have been taken in other contexts that relate to information.

3.224 When approaching this issue, it is important to bear in mind that an offence is only committed if the individual was within the scope of the Act in the first place. Therefore the effectiveness of any provision that extends the territorial ambit of the offence will be contingent upon the individual in question being brought within

[117] For example, see J Daskal, "The Un-territoriality of data" (2015) 125 *Yale Law Journal* 324.

[118] D Ormerod and D Perry (eds), *Blackstone's Criminal Practice* (2017), at B17.16 – B17.17.

[119] M Hirst, *Jurisdiction and the Ambit of the Criminal Law* (2003), p 224.

the scope of the legislation, either by being a Crown servant, government contractor or notified person.

Provisional Conclusion 16

3.225 **The territorial ambit of the offences contained in the Official Secrets Act 1989 should be reformed to enhance the protection afforded to sensitive information by approaching the offence in similar terms to section 11(2) of the European Communities Act 1972 so that the offence would apply irrespective of whether the unauthorised disclosure takes place within the United Kingdom and irrespective of whether the Crown servant, government contractor or notified person who disclosed the information was a British citizen. Do consultees agree?**

Public interest

3.226 A number of non-governmental stakeholders have made the suggestion that there ought to be a public interest defence in the Official Secrets Act 1989. Given the complexity of this issue, this will be considered in Chapter 7.

THE OPTIMAL LEGISLATIVE VEHICLE FOR REFORM

3.227 As our analysis has demonstrated, it is possible to envisage ways the legislation could be amended to deal with the discrete issues that stakeholders have brought to our attention. We believe, however, that it is necessary to consider the manner in which such changes could be introduced so as to maximise their effectiveness and signal that the law has changed.

3.228 There are a number of reasons why we believe a fundamental overhaul of the Official Secrets Act 1989 would be the optimal solution to the deficiencies that we have identified. These are mainly attributable to the fact that there are problems with the current law that cannot necessarily be remedied through targeted reform.

(1) As we discussed in the previous chapter, the title of the Official Secrets Acts does not accurately convey the distinct purposes of the legislation. The aim of the 1911 – 1939 Acts is to criminalise those who commit espionage. The aim of the 1989 Act, on the other hand, is to protect information that falls within specified categories. Despite the fact they have the same title, the aims of the legislation are distinct. Ideally, this would be demonstrated by their having different titles.

(2) The fact the Official Secrets Act 1989 refer to "secrets" gives an inaccurate impression of its aim and, we believe, means it is viewed with undue suspicion. The title of the legislation also means that it is unclear how far the criminal law extends. Other jurisdictions that have modernised legislation that is comparable to the Official Secrets Act 1989 have adopted more specific titles. In Canada, for example, the relevant legislation is entitled the "Security of Information Act". Arguably, this more accurately conveys the aim of the legislation, which is about ensuring information is secure, rather than about keeping it secret. We would welcome, however, consultees' views on whether the title of the legislation ought to change.

(3) Repealing the Official Secrets Act 1989 and replacing it with modern legislation would provide the opportunity not only to clarify what types of conduct are criminalised by the law, but also to re-educate those who work in the public sector on the nature of their legal obligations. Stakeholders have suggested that there may exist a misunderstanding surrounding what types of information are encompassed by the Official Secrets Act 1989. For example, there are those who still believe the 1989 Act criminalises the unauthorised disclosure of any information, rather than just information that falls within specific categories listed in the Act.

(4) There are practical reasons why fundamental reform could be preferable to amendments to effect the targeted reforms we described in previous sections. Specifically, it could be difficult to amend the legislation in the ways we suggest whilst retaining the current legislative framework. To take an example, it would be difficult to amend the offences in the Official Secrets Act 1989 in the way we suggest without amending other aspects of the legislation.

3.229 Similar views about the need for new legislation have been expressed in the past. For example, in 2004, the Security and Intelligence Committee of Parliament concluded that, "We believe the time has come to consider whether a new Act would be the proper way forward".[120] We agree with this conclusion.

3.230 Such an approach was also recommended by the Franks Committee, which concluded that a single "Official Information Act" was preferable to the multitude of offences that were then scattered throughout dozens of legislative provisions.

Provisional conclusion 17

3.231 **The Official Secrets Act 1989 ought to be repealed and replaced with new legislation. Do consultees agree?**

[120] Security and Intelligence Committee, 2003-2004 Annual Report (June 2004) Cm 6240, p 43. The Committee as currently constituted has expressed no view on the Official Secrets Acts 1911-1989.

CHAPTER 4
MISCELLANEOUS UNAUTHORISED DISCLOSURE OFFENCES

INTRODUCTION

4.1 As with the preceding chapters, this chapter is concerned with offences that criminalise the unauthorised disclosure of specified categories of information. Specifically, it considers those offences that are contained in legislation other than the Official Secrets Acts 1911-1939 or 1989. For convenience, these offences are collectively referred to as "miscellaneous unauthorised disclosure offences".

4.2 A large number of miscellaneous unauthorised disclosure offences have been introduced in an array of statutes and statutory instruments since at least the 1940s.[1] Our research has revealed the existence of 124 such offences, which we have listed in Appendix C.

4.3 The miscellaneous unauthorised disclosure offences fall broadly into two categories. The first category contains those offences which criminalise the disclosure of personal information held by public bodies, which we will refer to as "personal information disclosure offences". The second category contains those offences that criminalise the unauthorised disclosure of information concerning national security, such as information that relates to the enrichment of uranium, which we will refer to as "national security disclosure offences".

4.4 Our aim in this chapter is to describe the current legislative landscape and examine the extent to which there is uniformity in the form the offences take, the sentences available etc. As this chapter will demonstrate, despite the fact that these offences all appear to have the same general purpose, namely to criminalise the unauthorised disclosure of specified categories of information, they are not drafted in a uniform fashion. We will also examine the offence contained in section 55 of the Data Protection Act 1998. We have paid particular attention to section 55 because it is the best known and the most often invoked miscellaneous unauthorised disclosure offence. We conclude by seeking consultees' views on whether there is a need to undertake a more extensive review of the miscellaneous unauthorised disclosure offences identified.

4.5 At this stage it is important to point out that in our previous project on *Data Sharing* we recommended a law reform project ought to be undertaken that would be intended to facilitate the sharing of information within government (in addition to bodies carrying out tasks on behalf of government). Reform of the offences themselves would form part of providing more effective gateways. Whilst we still support such a project, as this chapter will demonstrate, we believe there is nevertheless merit in considering whether the offences could be reformed irrespective of reform of the gateways.

[1] There has been minimal commentary on these offences. For brief allusions see P Richardson (ed), *Archbold* (2016), ch 25 para 373; C Zietman, "Solicitors – Watching the Detectives" (1992) 89(30) *Law Society Guardian Gazette* 17.

PREVIOUS RECOMMENDATIONS FOR REFORM

4.6 The miscellaneous unauthorised disclosure offences examined in this chapter have previously been the subject of review. Three previous reviews which considered the offences are summarised below, the first was published by Justice and the British Committee of the International Press Institute in 1965; the second by the Franks Committee in 1972; and the third by the Information Commissioner's Office in 2006.

Justice and the British Committee of the International Press Institute

4.7 This assessment of miscellaneous unauthorised disclosure offences formed part of a broader review of the law and the press.[2] The establishment of the working party that undertook the review was not widely publicised and meetings with press representatives where held in private. This was to allow the press the opportunity to "speak freely and give concrete examples".[3]

4.8 The Working Party considered miscellaneous unauthorised disclosure offences briefly and in tandem with their review of section 2 of the Official Secrets Act 1911 (which has since been repealed).[4] They suggested that the miscellaneous unauthorised disclosure offences could be split into five main types.

(1) information that would be prejudicial to state security;

(2) information that would be prejudicial to the national interest;

(3) information that would allow opportunities for unfair financial gain;

(4) information given to the Government in confidence;

(5) information relating to government efficiency and integrity.[5]

4.9 The Working Party concluded that section 2 of the Official Secrets Act 1911 should apply to every category except information relating to government efficiency and integrity.[6] They reasoned that such an exemption would be too hard to draft. This led the Working Party to recommend a general defence encompassing consideration of the public interest:

2 Justice and the British Committee of the International Press Institute, *The Law and the Press* (1965).

3 Justice and the British Committee of the International Press Institute, *The Law and the Press* (1965) para 5.

4 On the replacement of section 2 of the 1911 Act with the Official Secrets Act 1989, see Chapter 3

5 Justice and the British Committee of the International Press Institute, *The Law and the Press* (1965) para 72.

6 For discussion of the repeal of the Official Secrets Act 1911, s 2 and its replacement with the Official Secrets Act 1989, see Chapter 3

> We therefore recommend that it should be a defence in any prosecution under the Official Secrets Act [1911] to show that the national interest or legitimate private interest confided to the State were not likely to be harmed and that information was passed and received in good faith and in the public interest.[7]

The Franks Committee

4.10 As we discussed in Chapter 3, the Franks Committee was formed "to review the operations of section 2 of the Official Secrets Act 1911 and to make recommendations".[8] As part of its review, the Committee assessed offences which criminalised the unauthorised disclosure of personal information.

4.11 The Committee maintained that such an assessment was necessary because personal information held by government could be left inadequately protected if, as they recommended, section 2 of the 1911 Act was repealed and replaced with a number of more specific offences. This was due to what the Committee saw as the inconsistent criminalisation of the unauthorised disclosure of personal information:

> For instance, census information is expressly protected by the Census Act, but there is no specific legal protection for income tax returns.[9]

4.12 The Committee maintained that the unauthorised disclosure of personal information held by government was worthy of criminalisation because:

(1) to function effectively government requires private citizens' information;

(2) citizens provide this information on the, either explicit or implicit, understanding that it will be held by government in confidence;

(3) the disclosure of the information would thus lead to a breakdown of trust between citizens and government; and

(4) such a breakdown could have "considerable adverse repercussion" for government and the nation.[10]

4.13 This view was strongly held. Indeed, the Committee stated:

> There is no tension in this sphere between openness and secrecy. There is no public interest in the disclosure of this information.[11]

[7] Justice and the British Committee of the International Press Institute, *The Law and the Press* (1965) para 74.

[8] *Departmental Committee on Section 2 of the Official Secrets Act 1911* (1972) Cmnd 5104, para i.

[9] *Departmental Committee on Section 2 of the Official Secrets Act 1911* (1972) Cmnd 5104, para 196.

[10] *Departmental Committee on Section 2 of the Official Secrets Act 1911* (1972) Cmnd 5104, para 197.

4.14 The same reasoning was not extended to information given in confidence to the private sector. The Committee did not believe that the same relationship of trust existed between consumers and businesses as existed between citizens and the state.[12]

4.15 Consequently, the Committee recommended the creation of a general offence that would criminalise the unauthorised disclosure of information provided to the Government by an individual or business.[13] Such information would not need to have been given in confidence. The offence would not apply to the private sphere, government contractors or those who received the protected information from a Crown servant.[14] It is unclear, however, whether the intent was to repeal the existing range of offences and replace them with a general offence that would apply in specified cases.

4.16 It would have been a defence under the proposed Official Information Act for a Crown servant to show either that:

(1) he reasonably believed that he was not acting contrary to his official duty; or

(2) he did not know and had no reason to believe that the document/information had been given by a private individual.[15]

4.17 A number of the recommendations the Committee made in relation to the offence that would have replaced section 2 of the Official Secrets Act 1911 were also recommended to apply to confidential information:

(1) the Attorney General's consent would be required before a prosecution could be initiated;[16]

(2) a maximum sentence in the Crown Court of two years' imprisonment and/or an unlimited fine;[17]

(3) a maximum sentence in a magistrates' court of six months' imprisonment and/or a maximum fine of £400;[18] and

[11] *Departmental Committee on Section 2 of the Official Secrets Act 1911* (1972) Cmnd 5104, para 200.

[12] *Departmental Committee on Section 2 of the Official Secrets Act 1911* (1972) Cmnd 5104, para 198.

[13] *Departmental Committee on Section 2 of the Official Secrets Act 1911* (1972) Cmnd 5104, para 278(12).

[14] For example, if a Crown servant disclosed the confidential information to a national newspaper who then published it, the newspaper would not have committed the offence.

[15] *Departmental Committee on Section 2 of the Official Secrets Act 1911* (1972) Cmnd 5104, Para 278(16).

[16] *Departmental Committee on Section 2 of the Official Secrets Act 1911* (1972) Cmnd 5104, para 278(25).

[17] *Departmental Committee on Section 2 of the Official Secrets Act 1911* (1972) Cmnd 5104, para 278(28).

(4) the creation of an offence of failing to take reasonable care of an official document.[19]

The Information Commissioner's Office

4.18 In May 2006 the then Information Commissioner,[20] Richard Thomas, laid a report before Parliament on the industry that had developed around the illegal trade in personal information.[21] The legal analysis in the report was focused upon section 55 of the Data Protection Act 1998 and only alluded briefly to other personal information disclosure offences.[22] In the report the Information Commissioner called for the disclosure offence in section 55 to be made imprisonable:

> The crime at present carries no custodial sentence. When cases involving the unlawful procurement or sale of confidential personal information come before the courts, convictions often bring no more than a derisory fine or a conditional discharge. Low penalties devalue the data protection offence in the public mind and mask the true seriousness of the crime, even within the judicial system. They likewise do little to deter those who seek to buy or supply confidential information that should rightly remain private. The remedy I am proposing is to introduce a custodial sentence of up to two years for persons convicted on indictment, and up to six months for summary convictions.[23]

4.19 Having laid the report before Parliament, the Information Commissioner's Office undertook consultation with interested stakeholders including the Government, media representatives, the financial industry, and professional bodies.[24] This led to a follow up report being laid before Parliament in December 2006.[25] This subsequent report echoed earlier calls for the offence contained in section 55 of the Data Protection Act 1998 to be made an imprisonable offence with a maximum sentence of two years' imprisonment and/or a fine.[26]

[18] *Departmental Committee on Section 2 of the Official Secrets Act 1911* (1972) Cmnd 5104, para 278(28).

[19] *Departmental Committee on Section 2 of the Official Secrets Act 1911* (1972) Cmnd 5104, para 278(17).

[20] For general information on the Information Commissioner and the Information Commissioner's Office see, Information Commissioner's Office, "About the ICO" https://ico.org.uk/about-the-ico/ (last visited 8 November 2016).

[21] Information Commissioner's Office, *What Price Privacy?* (2006).

[22] Information Commissioner's Office, *What Price Privacy?* (2006) para 7.7.

[23] Information Commissioner's Office, *What Price Privacy?* (2006) Richard Thomas' preamble 3.

[24] Information Commissioner's Office, *What Price Privacy Now*? (2006) 16-26.

[25] Information Commissioner's Office, *What Price Privacy Now*? (2006).

[26] Information Commissioner's Office, *What Price Privacy Now*? (2006) 27.

PERSONAL INFORMATION DISCLOSURE OFFENCES

4.20 Our research has revealed the existence of numerous offences that criminalise the unauthorised disclosure of personal information. Specifically, these personal information disclosure offences criminalise the unauthorised disclosure of information relating to identifiable individuals. This includes legal persons, such as corporations.

4.21 This section will examine these personal information disclosure offences. As our discussion below reveals, these offences are not drafted in a uniform fashion and there are considerable variations between them.

4.22 The vast majority of the miscellaneous unauthorised disclosure offences that our research has uncovered criminalise the unauthorised disclosure of personal information that has been supplied to a public body pursuant to a "legislative gateway". In 2014 we published a scoping report entitled *Data Sharing between Public Bodies* in which we described "legislative gateways" in the following terms:

> Legislative powers to share information are often referred to as "gateways". They may be express powers, conferring power to share information, perhaps for a particular purpose, or with a particular public body. Alternatively, the power may be implied, where data sharing is reasonably incidental to an express power to do something else. Throughout this report we use the term "gateway" to describe a statutory provision empowering (or, more rarely, requiring) a public body to disclose information held by it to another, usually also public, body. These provisions can be accompanied by criminal offences of unauthorised disclosure on the part of staff of the disclosing body and sometimes of unauthorised further disclosure by staff of the recipient body. They can contain provisions circumscribing the categories of information that may be disclosed and/or the circumstances in which, or purposes for which, it may be disclosed.[27]

4.23 As stated above, a list of the miscellaneous unauthorised disclosure offences that our research has revealed is included in Appendix C. These offences will be considered across the key themes listed below.

(1) The type of conduct the offence criminalises.

(2) The fault element of the offences.

(3) The extent to which the recipient of the information is criminalised for his or her conduct.

(4) Statutory defences and exemptions.

(5) Requirements to prosecute.

(6) Maximum sentences.

[27] Data Sharing between Public Bodies a Scoping Report (2014) LC No 351 para 1.35.

4.24 The aim in examining these inconsistencies is to assess the extent to which personal information disclosure offences form a rational scheme of protection.

The type of conduct criminalised by the offence

4.25 A typical example of the structure of personal disclosure offences is section 8 of the Mesothelioma Act 2014:

> (1) A person involved in the administration of the [Diffuse Mesothelioma Payment] scheme must not, without lawful authority, disclose information which—
>
> > (a) was acquired in connection with the administration of the scheme, and
> >
> > (b) relates to a particular person who is identified in the information or whose identity could be deduced from it.

4.26 Rather than applying to anyone who handles personal information, these offences are usually targeted at specific groups of public sector employees. For example, the above offence in the Mesothelioma Act can only be committed by a person involved in the Diffuse Mesothelioma Payment Scheme. Similarly, section 23 of the Civil Aviation Act 1982 criminalises the disclosure of personal information, but its applicability is limited to the Civil Aviation Authority, its employees and its members.

4.27 There is a lack of uniformity across the legislative landscape as to what form of conduct constitutes a criminal offence. Most of the offences only criminalise the unauthorised *disclosure* of information.[28] The offence in section 55 of the Data Protection Act 1998, however, can be committed not only by disclosing information, but also by obtaining it or by procuring its disclosure by someone else.

4.28 These textual differences may have significant implications for the extent to which personal information is protected in practice. The following example demonstrates this point:

> A solicitor instructs a private investigator to find out information about a person who is divorcing one of his clients. Consequently, the private investigator "blags" personal data concerning the person from an employee of the Director of Public Prosecutions. The relevant information concerns child support. The private investigator then passes this information on to the solicitor.[29]

[28] Though the section 55 offence is not the only example of an offence which criminalises beyond disclosure. Section 102 of the Tribunals, Courts and Enforcement Act 2007 also criminalises the unauthorised use of information.

[29] "Blagging" refers to obtaining personal information from data controllers through deception. See further P Carey, *Data Protection: A Practical Guide to UK and EU Law* (2015) p 250.

4.29 The disclosure offence in section 129 of the Welfare Reform Act 2012 criminalises the unauthorised disclosure of social security information which was provided to the Director of Public Prosecutions by the Secretary of State pursuant to section 128 of the 2012 Act. In relation to the offence contained in section 129 of the 2012 Act, the only person in the above example who would have committed a criminal offence is the employee of the Director of Public Prosecutions. This is because the offence is framed so as to relate only to a narrow category of people and can only be committed by way of a disclosure. Comparatively, the offence in section 55 of the Data Protection Act 1998 is sufficiently broad to encompass the employee in question in addition to the private investigator who obtained the information and the solicitor who procured the disclosure of the information.[30]

Fault element

4.30 Most of the personal information disclosure offences are offences of strict liability. This means there is no requirement to prove that an individual had a specific state of mind when he or she disclosed the information in question before liability can be imposed. Yet a small number of the personal information disclosure offences do explicitly include a fault element as to both consequences and circumstances. Within this minority there is variance as to what standard of fault is required and to what conduct this fault element corresponds.

4.31 By way of an example of this inconsistency, the offence in section 55 of the Data Protection Act 1998 criminalises reckless disclosure. This means that and individual commits an offence where he or she obtains, discloses or procures an unauthorised disclosure (conduct element) and does so either knowing or being reckless as to whether he or she is authorised to make such a disclosure (circumstance element). By way of contrast, an individual only commits an offence contrary to section 9 of the Rehabilitation of Offenders Act 1974 if he or she discloses information (conduct element) and he or she knows or has reasonable cause to suspect that any specified information obtained in the course of those duties is specified information (circumstance element). Section 9(2) provides:

> Subject to the provisions of any order made under subsection (5) below, any person who, in the course of his official duties, has or at any time has had custody of or access to any official record or the information contained therein, shall be guilty of an offence if, knowing or having reasonable cause to suspect that any specified information he has obtained in the course of those duties is specified information, he discloses it, otherwise than in the course of those duties, to another person.

[30] For more detailed discussion of when the law firm and the private investigator may be liable see A Roughton and D Heward-Mills, "Dirty work -- Criminal Aspects of Bin Trawling" (2009) 9(5) *Privacy and Data Protection* 12; C Evans, "The Offence in Section 55 DPA -- Unlawful Obtaining of Personal Data" (2003) 3(6*) Privacy and Data Protection* 3. For a comment on an unreported case where private investigators were convicted of conspiracy to defraud rather than section 55 of the 1998 Act see "Private Eyes Who Stole Confidential Information for Profit Sent to Prison" (2012) 17(4) *Communications Law* 4.

4.32 This example demonstrates a further lack of uniformity in how the offences are drafted, namely the circumstance element to which the fault element attaches. In the former example the fault element is directed toward the manner in which disclosure is made and in the latter to the type of information being disclosed.

The extent to which the recipient of the information is criminalised

4.33 A small number of the personal information disclosure offences criminalise those who receive the information that was disclosed without authorisation if they in turn disclose the information without lawful authority.

4.34 There is significant inconsistency between the personal information disclosure offences as to whether the offence can be committed by someone other than the individual who disclosed the information. Some offences explicitly criminalise onward disclosures. For example, the disclosure offence in section 39 of the Statistics and Registration Service Act 2007 can be committed by members and employees' of the Statistics Board and by "any other person who has received [the information] directly or indirectly from the Board".

4.35 There are other personal information disclosure offences, however, that have complete exemptions if there has been a previous disclosure. Such an exemption is included in schedule 11 to the Local Audit and Accountability Act 2014, which provides that "this paragraph does not prohibit the disclosure of information if the information is or has been available to the public from any other source".

4.36 There is a third set of personal information offences which exempt disclosures if they have previously been made lawfully. Such an exemption applies to the disclosure offence in section 3 of the Television Licences (Disclosure of Information) Act 2000, which provides: "(3) It is not an offence under this section– … (b) to disclose information which has previously been disclosed to the public with lawful authority".

4.37 Other personal information disclosure offences neither explicitly apply to, nor exempt, subsequent disclosures. An example of this is the offence in schedule 22 of the National Health Service Act 2006:

> No person who *obtains any information by virtue of* section 260 or this Schedule may, otherwise than in connection with the execution of that section or this Schedule or of an order made under that section, disclose that information except… (emphasis added)

4.38 This lack of uniformity makes it difficult to ascertain why it was deemed appropriate to criminalise, or not criminalise, someone other than the individual who disclosed the information in question.

Statutory defences and exemptions

4.39 The majority of the personal information disclosures offences our research has uncovered do not have corresponding statutory defences. It would nonetheless still be possible to plead a common law defence, such as duress.

4.40 For those offences that are accompanied by a statutory defence, the most common is that the individual who disclosed the information reasonably believed he or she had lawful authority to do so.[31] Other available statutory defences include: having a reasonable belief that the information was already publicly available;[32] due diligence;[33] reasonable belief in having authority to disclose with no reasonable cause to believe otherwise;[34] that the disclosure was either of publicly available information or the discloser reasonably believed this to be the case;[35] and that the disclosure was to protect the welfare of an individual or the discloser reasonably believed this to be the case.[36]

4.41 Although statutory defences are rare, nearly every personal information offence our research has uncovered contains corresponding statutory exemptions. The primary practical difference between defences and exemptions lies in the evidential burden placed upon the defendant. Under section 101 of the Magistrates' Court Act 1980, defendants who seek to rely on a statutory exemption must prove it to a legal standard.[37] In other words, the defendant must show that on the balance of probabilities he or she satisfies the criteria for exemption. By way of contrast, defences typically only require the issue to be raised by the defence to an evidential standard. This means he or she merely has to adduce sufficient evidence to raise the defence as an issue. The burden then shifts to the prosecution to prove beyond reasonable doubt that the defence does not apply.

4.42 Common exemptions include disclosure:

(1) with the consent of the person to whom the information related;[38]

(2) for the purposes of criminal or civil proceedings;[39]

(3) to satisfy an international obligation;[40]

(4) after the death of the person to whom the information related;[41]

(5) for the purpose of a criminal investigation;[42]

[31] See for example, Child Support Act 1991, s 50.

[32] See for example, Welfare Reform Act 2012, s 129.

[33] See for example, Financial Services and Markets Act 2000, s 352.

[34] See for example, Social Security Administration Act 1992, s 123.

[35] See for example, Health and Social Care Act 2008, s 77.

[36] See for example, Health and Social Care Act 2008, s 77.

[37] For discussion of both how the Magistrates' Court Act 1980 can extend to either way offences and the human rights implications of the Act see D Ormerod and D Perry (eds), *Blackstone's Criminal Practice* (2017) para F3.11 and following.

[38] See for example, Pensions Act 2004, s 82.

[39] See for example, Enterprise Act 2002, s 245.

[40] See for example, Merchant Shipping (Liner Conferences) Act 1982, s 10.

[41] See for example, Railways Act 1993, s 145.

[42] See for example, Welfare Reform Act 2012, s 129.

(6) to a particular person or body for a purpose allowed by statute or statutory instrument;[43]

(7) in response to a request under the Freedom of Information Act 2000;[44]

(8) after previous lawful disclosure;[45] and

(9) after previous disclosure.[46]

4.43 A fairly standard example is section 10 of the Merchant Shipping (Liner Conferences) Act 1982:

> (2) Information obtained by the Secretary of State as appropriate authority for the purposes of the Code shall not, without the consent of the person from whom it was obtained, be disclosed except—
>
> > (a) for the purpose of the discharge by the Secretary of State of his functions in connection with the Code; or
> >
> > (b) for the purpose of any proceedings arising out of the Code; or
> >
> > (c) with a view to the institution of, or otherwise for the purposes of, any criminal proceedings, whether under this Act or otherwise; or
> >
> > (d) to an EU institution in pursuance of a EU obligation;[47]

4.44 On occasion, what constituted an exemption in one statute appears as a defence in another.[48] Some offences contain more distinctive exemptions. For example, section 32 of the Chemical Weapons Act 1996 contains exemptions for both "dealing with an emergency involving danger to the public" and "with a view to ensuring the security of the United Kingdom". Such exemptions are unusual, however, and are context specific.

[43] See for example, Construction Products Regulations 2013/1387, reg 22.

[44] See for example, Defence Reform Act 2014, sch 5.

[45] See for example, Legal Aid, Sentencing and Punishment of Offenders Act 2012, s 33.

[46] See for example, Local Audit and Accountability Act 2014, sch 11.

[47] As amended by Treaty of Lisbon (Changes in Terminology) Order 2011/1043 art 6(1).

[48] Compare the defence contained in the Health and Social Care Act 2008, s 77 to the exemptions in the Merchant Shipping (Liner Conferences) Act 1982, s 10 which are listed above.

Consent before a prosecution can be commenced

4.45 A minority of the personal information offences require the consent of the Director of Public Prosecutions or some other specified individual before a prosecution can be commenced.[49] Other office holders who must consent before a prosecution for some of the other specific disclosure offences may be initiated includes the Secretary of State;[50] the Natural Resources Body for Wales;[51] and the Information Commissioner.[52] There is therefore an inconsistency within the personal information disclosure offences as to whether a prosecution can only be commenced with consent.

Maximum sentences

4.46 The maximum sentence for most of the personal disclosure offences uncovered by our research is two years' imprisonment and/or a fine.[53] Some offences have higher maximum sentences. The maximum sentences available for the personal information disclosure offences uncovered by our research range from a fine only, to five years' imprisonment. Our research has not revealed a definitive explanation as to why the maximum sentences for offences that criminalise the unauthorised disclosure of similar categories of information ought to vary to such a large extent. One explanation is that the disclosure of personal information is deemed to be more serious in some contexts than in others. It is important to note, however, that maximum sentence is only one indicator of seriousness.

DIGITAL ECONOMY BILL

4.47 The above described inconsistencies between personal information disclosure offences need to be considered in light of the Digital Economy Bill.[54] The Bill makes provision for the creation of a number of legislative gateways, which we defined earlier.

4.48 The explanatory notes to the Bill explain one of its aims in the following terms:

> For a public authority to access information held in another part of the public sector it requires appropriate legal powers, which are often provided by express legal gateways to disclose information. The government believes that the current legal landscape of data sharing for public service delivery is unduly complex and inconsistent across public services and organisations. This may hinder the ability of public authorities to offer citizens timely and appropriate interventions and to respond quickly to a changing social and policy environment.

[49] For example, Commissioners for Revenue and Customs Act 2005, s 19. By virtue of section 1(7) of the Prosecution of Offences Act 1985 the consent of the Director of Public Prosecutions can be given by any prosecutor.

[50] Companies Act 2006, ss 459-460.

[51] Health and Safety at Work etc. Act 1974, s 38.

[52] Data Protection Act 1998, s 59.

[53] For example, Water Resources Act 1991, s 204.

[54] The Digital Economy Bill is currently at the committee stage in the House of Lords.

> The Bill provides a single gateway to enable public authorities, specified by regulation, to share personal information for tightly constrained reasons agreed by Parliament, where its purpose is to improve the welfare of the individual in question. To use the gateway, the proposed sharing of information must be for the purpose of one of the specified objectives, which will be set out in regulations. [55]

4.49 According to a consultation paper published in 2016 by the Cabinet Office, entitled *Better Use of Data*, the provisions in the Bill are designed to coexist with, rather than override, the provisions that currently permit public authorities to share information.[56]

4.50 The paper indicates that the new unauthorised disclosure offences contained in the Bill are intended to supplement those offences already found in section 19 of the Commissioners for Revenue and Customs Act 2005; section 123 of the Social Security Administration Act 1992; section 50 of the Child Support Act 1991; and section 39 of the Statistics and Registration Service Act 2007. In keeping with this aim the Bill does not repeal any of the legislative gateways that are currently in force or the criminal offences that accompany them.

4.51 As will be apparent from the preceding analysis, these are not the only personal information disclosure offences that currently exist. It is therefore conceivable that the criminal offences contained in the Bill will overlap with other offences that already exist.

A POSSIBLE EXPLANATION FOR THE INCONSISTENCIES BETWEEN PERSONAL INFORMATION DISCLOSURE OFFENCES

4.52 It is possible that there is good reason for the degree of inconstancy between the formulations of the personal information disclosure offences that we have examined in previous sections. As a starting point, the breadth of what can constitute "personal information" must be acknowledged. The term could extend from a name, on the one hand, to a person's bank details and address on the other. Given this breadth, it is conceivable that those offences with more restrictive conditions (such as those that criminalise the recipients of information disclosed without lawful authority) have been created in contexts where more sensitive personal information could be disclosed, such as a person's bank details. This hypothesis can draw support from the aforementioned Cabinet Office paper in which it is stated that:

> To protect against the unlawful disclosure of data, it is proposed that a new criminal offence for unlawful disclosure is introduced.

[55] Available at http://www.publications.parliament.uk/pa/bills/cbill/2016-2017/0045/en/17045en.pdf (last visited 9 November 2016).

[56] Available at https://www.gov.uk/government/consultations/better-use-of-data-in-government (last visited 9 November 2016).

> To reflect the fact that there is greater sensitivity with respect to data held by HMRC, additional safeguards in line with existing disclosure models are proposed to protect HMRC data once it has left the department. This ensures that HMRC still retains discretion on any proposed further uses and disclosures of HMRC information, and that unless specifically authorised, the recipient may not exceed what HMRC would be able to disclose, if approached directly for information.[57]

4.53 Without a more extensive review, however, we are unable to come to a conclusion on whether this rationale can apply to all disclosure offences uncovered by our research.

CONCLUSION ON PERSONAL INFORMATION DISCLOSURE OFFENCES

4.54 In this section we have examined those offences that criminalise the unauthorised disclosure of personal information. As our analysis has demonstrated, the legislative landscape is far from uniform. Many of these offences accompany legislative gateways, which makes the lack of uniformity across the legislative landscape all the more surprising.

4.55 As we explained above, the provisions contained in the Digital Economy Bill do not streamline the legislative landscape, but rather add to it. From a theoretical perspective the legislative landscape looks irrational, dispersed and lacking in uniformity.

4.56 Such theoretical problems may well have practical implications. Difficulties could arise, for example, if the same category of information was encompassed by two separate offences. Such a result is a natural consequence of legislative gateways themselves often overlapping.[58] The potential for the offences to overlap is likely to be increased when the Digital Economy Bill receives the Royal Assent. As explained above, the offences contained within the Bill are not intended to replace existing offences. If one offence contained a defence, whilst the other did not, this could seem arbitrary without further explanation.

4.57 For example, section 55(2)(d) of the Data Protection Act 1998 provides a defence for the unauthorised disclosure of personal data if a defendant can prove that obtaining, disclosing or procuring personal data was justified as being in the public interest. On the other hand, clause 33 of the Digital Economy Bill would introduce a criminal offence for the unlawful disclosure of personal information, however, the clause does not provide a defence where the disclosure is in the public interest.

[57] Available at https://www.gov.uk/government/consultations/better-use-of-data-in-government (last visited 9 November 2016).

[58] For further comment on the extent of the overlap of existing legislative gateways see our earlier report on data sharing.

4.58 During our initial consultation with stakeholders, it was not suggested that the offences we have examined in this section were causing pressing problems in practice. Given the constraints of time, we have focused on those provisions that were characterised as being particularly problematic. These were considered in previous chapters. We are nonetheless of the view that the offences examined in this section are in need of a fuller review. This provisional conclusion parallels the conclusions in our 2014 Report, *Data Sharing Within Public Bodies*, in which we concluded:

> A strong argument can be made for reviewing the use of wrongful disclosure offences in relation to information disclosure. Consultees consistently expressed greater fears of criminal liability than we felt were justified. The fragmentary and inconsistent existence of wrongful disclosure offences may be part of the cause of this and this may benefit from rationalisation and simplification.

Consultation question 10

4.59 **Do consultees have a view on whether a full review of personal information disclosure offences is needed?**

SECTION 55 OF THE DATA PROTECTION ACT 1998

4.60 Perhaps the best known miscellaneous unauthorised disclosure offence is the offence contained in section 55 of the Data Protection Act 1998.[59] Section 55 makes it an offence knowingly or recklessly to obtain, or to procure the disclosure to another of personal data without the consent of the data controller.[60] This is a freestanding offence in the sense that, unlike most of the offences examined in the above section, it does not accompany a statutory information gateway. The offence can be committed by individuals in both the public and private sectors. As only the former would be holding official information under our definition of the term they shall be central to the following analysis.

4.61 Section 1(1) of the 1998 Act defines "personal data" as:

> Data which relate to a living individual who can be identified (a) from those data, or (b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.[61]

4.62 Section 1(1) also defines a "data controller" as:

[59] The offence is contained in s 55(3).

[60] For consideration of the meaning of both 'knowingly' and "recklessly" see D Ormerod and K Laird, *Smith and Hogan's Criminal Law* (14th ed 2015) pp 113-160.

[61] Section 1(1) was interpreted narrowly in *Durant v Financial Services Authority* [2003] EWCA Civ 1746, [2004] FSR 28 at [21]-[31], by Lord Justice Auld.

> A person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed.[62]

4.63 It is worth noting that, strictly speaking, the "victim" of the offence is not the person to whom the information relates (the data subject), but instead the data controller.[63] To take an example, in *Rooney* the appellant worked for Staffordshire Police and had the authority to access the personal information of staff for work purposes. The appellant's sister, AR, had a relationship and child with another Staffordshire police officer, AS. Their relationship deteriorated and ended. AS then started a relationship with another woman and they set up home together. The appellant accessed the personal data of AS and disclosed it to her sister. It was held on appeal that this constituted the unlawful disclosure of personal data. For present purposes the important point to note is that the victim was not the police officer whose personal data was disclosed, but Staffordshire Police, in its capacity as the data controller.[64]

4.64 Unlike most statutory offences, section 55 includes four defences:

(1) That the disclosing, obtaining or procuring was

(a) necessary to prevent or detect a crime; or

(b) required or authorised by law.

(2) That the defendant reasonably believed he or she had the right to obtain, disclose, or procure the disclosure to another of the information.

(3) That the defendant reasonably believed the data controller would have consented had he or she known of the disclosing, obtaining or procuring.

(4) In the circumstance the disclosing, obtaining, or procuring was in the public interest.[65]

[62] For discussion see P Carey with B Treacy, *Data Protection* (4th ed 2015) pp 29-30.

[63] In *What Price Privacy*? the Information Commissioner's Office accepted this: Information Commissioner's Office, *What Price Privacy: the Unlawful Trade in Confidential Personal Information* (2006) para 3.10. The report repeatedly conceptualises the data subject as the victim. For example the first line of Richard Thomas' foreword (page 3), then Information Commissioner, is "Protecting the privacy of the individual goes to the heart of my responsibilities under data protection legislation".

[64] *R v Rooney* [2006] EWCA Crim 1841.

[65] Public interest defences to unauthorised disclosure offences are specifically considered in Chapter 7.

4.65 The maximum sentence on conviction, either summarily or on indictment, is an unlimited fine.[66] Initial consultation with stakeholders has suggested that in practice fines rarely exceed £1,000. For example, in *Rooney*, which was heard in the Crown Court, a fine of £700 was imposed.[67] When giving evidence to the House of Commons Justice Select Committee in 2011, Christopher Graham, the then Information Commissioner, referenced a case before a magistrates' court where a fine of £800 was imposed.[68] Morrison has described the fines that have historically been imposed as "relatively meagre".[69] Similarly, Townsend and Southern have commented, that, "fines issued in the last year tend to be in the hundreds rather than the thousands of pounds".[70]

4.66 Two important reforms to section 55 of the Data Protection Act 1998 Act were included in the Criminal Justice and Immigration Act 2008. First, section 77 of the 2008 Act gives the Secretary of State the power to make section 55 of the 1998 an imprisonable offence with a maximum sentence of 12 months' imprisonment and/or a fine on conviction in the magistrates' court; and two years' imprisonment and/or a fine on conviction in the Crown Court. Before exercising the power to bring this provision into force, the Secretary of State must consult with the Information Commissioner, appropriate media organisations and other appropriate persons.[71] Although section 77 of the 2008 Act has been granted the Royal Assent, the Secretary of State has not yet exercised the power to bring it into force.

4.67 Secondly, section 78 of the 2008 Act inserts a new statutory defence into section 55 of the Data Protection Act 1998. This defence may be pleaded if the individual who disclosed the personal data was acting with a view to publishing "journalistic, literary or artistic material"; and with the reasonable belief that the disclosure, obtaining or procuring was in the public interest. Section 78 is not yet in force.[72]

[66] An unlimited fine is only available on summary conviction for offences committed after 13 April 2015. On that date the Legal Aid, Sentencing and Punishment Act 2012, s 85 came into force. Offences committed before this date which are tried summarily under the 1998 Act, s 55 will retain the previous maximum sentence of £5,000. See, *Ministry of Justice, Criminal Justice and Courts Act 2015 Circular No. 2015/01* (2015) p 11.

[67] *R v Rooney* [2006] EWCA Crim 1841 at [1] and [16], by Mr Justice Bean.

[68] For comment, see B Treacy, "Commissioner's Evidence to the House of Commons – Analysis" (2011) 12 *Privacy and Data Protection* 7.

[69] T Morrision, "Getting Off Lightly?" (2008) 158 *New Law Journal* 645.

[70] L Townsend and V Southern, "The Cost of Non-compliance with Data Protection Law" (2006) 6(7) *Privacy and Data Protection* 9.

[71] Criminal Justice and Immigration Act 2008, s 77(4).

[72] Brimsted suggests that that the public interest defence for journalists was introduced as a result of press lobbying which in turn was triggered by the move to make the section 55 offence imprisonable. See K Brimsted, "Controllers vs. Processors — Useful Distinctions, or Distracting Labels?" (2008) 9(3) *Privacy and Data Protection* 2. For further consideration of this defence and public interest defences to disclosure offences more generally see Chapter 7.

4.68 Prosecutions under section 55 of the Data Protection Act 1998 can only be brought by the Information Commissioner, or by the Crown Prosecution Service with the consent of the Director of Public Prosecutions.[73]

4.69 The following sub-sections will examine some of the problems we have identified that relate specifically to the Data Protection Act 1998.

Maximum sentence

4.70 Despite the fact that the offence in section 55 of the Data Protection Act 1998 can be tried in both a magistrates' court and in the Crown Court, the maximum available sentence for the offence is a fine. As the previous section demonstrated, a number of commentators have expressed the view that this maximum sentence is not commensurate with the seriousness of the harm that can be caused by the disclosure of such data. Stakeholders expressed the same viewpoint during our initial consultation.

4.71 Despite the fact that the maximum available sentence is a fine, there are a number of judgments in which the courts have stated that the disclosure of personal data constitutes a serious offence. For example, in *Attorney General's Reference*, Lord Justice Judge remarked:

> The unauthorised disclosure of information held in any record kept and maintained only for public purposes should always be regarded as a serious offence.[74]

4.72 Similarly, in *Rooney*, Mr Justice Bean stated:

> The police are entitled to regard the unlawful use of information contained in personal data on police computers as a serious matter.[75]

4.73 The rise of the internet has significantly increased the amount of personal information which can be disclosed with relative ease. This was well demonstrated in 2007 when an employee of Her Majesty's Revenue and Customs lost two computer discs containing personal information relating to 25 million individuals including names, dates of birth, addresses, national insurance numbers, and bank account details.[76]

[73] Data Protection Act 1998, s 60. In effect the consent of the Director can be given by any crown prosecutor due to the Prosecution of Offences Act 1989, s 1(7).

[74] *Attorney General's Reference No 140 of 2004* [2004] EWCA Crim 3525 at [9], by Lord Justice Judge.

[75] *R v Rooney* [2006] EWCA Crim 1841 at [1] and [16], by Mr Justice Bean.

[76] Patrick Wintour, "Lost in the Post - 25 Million at Risk after Data Discs Go Missing" (*The Guardian*, 21 November 2007) http://www.theguardian.com/politics/2007/nov/21/immigrationpolicy.economy3 (last visited 8 November 2016). For an informative blog post on the limitations of the offences in the Data Protection Act 1998 in the context of large scale data loss see Dean Armstrong and Christopher Saad, "Data Protection: The Criminal Offences" http://www.2bedfordrow.co.uk/data-protection-the-criminal-offences/ (last visited 8 November 2016).

4.74 Individuals can now disclose large quantities of personal information instantaneously, causing harm to millions of people. It is questionable whether a maximum sentence of even two years' imprisonment could appropriately reflect the harm done by an intentional and large scale disclosure of personal information, especially if it is done for financial gain.

4.75 Our research has demonstrated the existence of cases in which an imprisonable offence was prosecuted instead of the offence in section 55, even when the latter could have been charged. In *Attorney General's Reference No 140 of 2004*, for example, the defendant was charged with misconduct in public office after disclosing personal information.[77] Lord Justice Judge explicitly commented that the behaviour also fell within the scope of the offence in section 55:

> The general count identified 13 individual occasions, which particularised the misconduct alleged, and related to obtaining the personal data of the keepers of 13 motor vehicles without the consent of the controller of the data, contrary to section 55(3) of the Data Protection Act 1998.[78]

4.76 Similarly, in *Summers*, the defendants were prosecuted for conspiracy to defraud in circumstances when they could have been prosecuted for an offence contrary to section 55 of the 1998 Act.[79]

4.77 Our initial consultation with stakeholders leads us to conclude that such cases are part of a more general trend whereby the low penalty available for the section 55 offence is circumvented by charging another criminal offence. It is undesirable that reliance should have to be placed upon other offences to compensate for the fact that the maximum penalty available for the offence in section 55 does not reflect the harm caused by the disclosure of personal data or the culpability of those who disclose it. This is despite the fact that the wrongdoing falls squarely within what section 55 is intended to punish.

4.78 As we discussed above, the Secretary of State can raise the sentence for the section 55 offence to a maximum sentence of two years' imprisonment, but is yet to do so.[80] It is worth reconsidering whether even a two year maximum sentence reflects the serious harm that can be caused by disclosing personal information.

Misdescribing the victim

4.79 As we have already discussed, the offence in section 55 of the Data Protection Act 1998 implies that the data controller is the victim of the unauthorised disclosure, rather than the individual whose personal data has been disclosed. This interpretation of the offence has been confirmed by the Information Commissioner's Office:

[77] *Attorney General's Reference No 140 of 2004* [2004] EWCA Crim 3525.

[78] *Attorney General's Reference No 140 of 2004* [2004] EWCA Crim 3525 at [1], by Lord Justice Judge LJ.

[79] *R v Summers (Daniel)* (2012) (unreported). For comment see "Private Eyes Who Stole Confidential Information for Profit Sent to Prison" (2012) 17(1) *Communications Law* 4.

[80] Criminal Justice and Immigration Act 2008, s 77.

> Technically the law looks on the organisation whose data has been captured (the data controller) as the 'victim' of the crime, rather than the individual whose details have been stolen (the data subject). In terms of the penalty imposed, the law makes no distinction between offences relating to sensitive or other personal data.[81]

4.80 We concur with the view of the Information Commissioner's Office that the offence is presently structured to make the data controller the victim. In support of this conclusion we would add that only the data controller can authorise a disclosure, but the consent of the data subject is not mentioned.[82]

4.81 It is peculiar that the person to whom the data relates, who is referred to in the legislation as the data subject, is not clearly conceptualised as the victim of the offence. It is information about him or her that has been disclosed without authority. This formulation of the offence certainly does not align with the Information Commissioner's Office's view of what the purpose of the offence ought to be. This is apparent from a report published in 2006 entitled *What Price Privacy?* in which Richard Thomas, the then information Commissioner, begins the paper by commenting "Protecting the privacy of the individual goes to the heart of my responsibilities under data protection legislation".[83] Thomas has also commented elsewhere that he prefers to refer to data protection as "people protection".[84] Yet this is not reflected in the way the offence is drafted.

4.82 Our initial consultation and research suggests that the data subject does have a quasi-victim status in practice. Stakeholders have confirmed that on occasion the data subject will submit evidence about the impact the disclosure had on him or her. Similarly, the judiciary has accepted that the impact of the breach on the data subject is important. For example, in *Attorney General's Reference No 140 of 2004*, Lord Justice Judge commented, "the impact of disclosure on any individual whose privacy has been betrayed is a critical ingredient of the sentencing decision".[85]

4.83 Although efforts to assess the impact of the disclosure on the data subject are welcome, they cannot alter the fact that he or she is not the victim for the purposes of the offence. We believe this suggests that the offence is in need of reformulation.

[81] Information Commissioner's Office, *What Price Privacy?* (2006) para 3.11.

[82] Data Protection Act 1998, s 55(1).

[83] Information Commissioner's Office, *What Price Privacy?* (2006) 3.

[84] Richard Thomas, "Individuals Value Their Privacy – Institutions Do Not" (22 November 2007, the Independent) http://www.independent.co.uk/voices/commentators/richard-thomas-individuals-value-their-privacy-institutions-do-not-759001.html (last visited 8 November 2016).

[85] *Attorney General's Reference No 140 of 2004* [2004] EWCA Crim 3525 at [9].

Conclusion on section 55 of the Data Protection Act 1998

4.84 The offence contained in section 55 of the Data Protection Act 1998 is problematic for a number of reasons. Some of these undermine the ability of the offence adequately to protect personal data. Whilst repealing and redrafting the offence might seem superficially attractive, such an approach could cause problems in practice. These are attributable to the fact that the offence is intended to supplement the other provisions in the Data Protection Act 1998. Repealing the offence might undermine the coherence of the Data Protection Act 1998 without necessarily remedying the defects with the offence contained in section 55. Given the problems we have identified with the offence, our provisional conclusion is that section 55 requires more extensive review to assess the extent to which it adequately protects personal information.[86]

Consultation question 11

4.85 **Do consultees have a view on whether the offence in section 55 of the Data Protection Act 1998 ought to be reviewed to assess the extent to which it provides adequate protection for personal information?**

NATIONAL SECURITY DISCLOSURE OFFENCES

4.86 The label "national security disclosure offence" encompasses those offences that criminalise the unauthorised disclosure of information that relates to national security. Our research has revealed the existence of only a small number of offences of this type. The offences we have chosen to focus on illustrate the issues are those dealing with, namely disclosures of information concerning nuclear energy and uranium;[87] and information useful to an enemy.[88] The offences in both of these categories are worth addressing in turn because they are formulated in quite distinct ways both from each other and from the offences in the Official Secrets Act 1989.

Nuclear energy and uranium

4.87 Our research has revealed the existence of five disclosure offences that relate to nuclear energy. First, section 11 of the Atomic Energy Act 1946 makes it an offence for a person to disclose information related to atomic energy plants without authority, if "to his knowledge" it is information of this type. Onward disclosure of information which has already been authorised to be in the public domain is not an offence. Secondly, section 13 of the 1946 Act criminalises the unauthorised disclosure of information obtained through powers granted by the Act. For example, this would cover information obtained by inspectors acting under powers granted in section 5 of the Act.

[86] Although the offence in section 55 contains a number of deficiencies, we believe it is also worthy of note that it does demonstrate that it is possible to craft an overarching offence that protects personal information.

[87] Anti-terrorism, Crime and Security Act 2001, s 79; Uranium Enrichment Technology (Prohibition on Disclosure) Regulations 2004/1818 brought into force by virtue of Anti-terrorism, Crime and Security Act 2001, s 80; and Nuclear Industries Security Regulations 2003/403, regs 22 and 25.

[88] Armed Forces Act 2006, ss 1 and 17.

4.88 Both of these offences can be tried in either the Crown Court or a magistrates' court.[89] If tried in the Crown Court, the maximum penalty is five years' imprisonment and/or a fine. If tried in a magistrates' court, the maximum sentence is three months' imprisonment and/or a fine. A prosecution under section 11, but not section 13, requires the consent of the Director of Public Prosecutions.[90] There are special sentencing provisions for corporate bodies.[91]

4.89 Thirdly, section 79 of the Anti-terrorism, Crime and Security Act 2001 criminalises the unauthorised disclosures of information that relates to nuclear security. The drafting of the offence means that subsequent disclosures are also encompassed by the offence. The maximum sentence is seven years' imprisonment and/or a fine if tried in the Crown Court. The offence applies to individuals in the United Kingdom and to citizens of the United Kingdom abroad. This extra-territorial effect is unusual, as most of the disclosure offences our research has revealed can only be committed if the individual is in the United Kingdom.

4.90 Fourthly, regulations made in accordance with section 80 of the Anti-terrorism, Crime and Security Act 2001 criminalise the unauthorised disclosure of specified categories of information relating to uranium enrichment technology.[92] As with section 79 of the Anti-Terrorism, Crime and Security Act 2001, this offence extends to individuals in the United Kingdom and to United Kingdom citizens abroad.[93] To commit the offence a person must disclose relevant equipment, software, or information. They must do so with:

> The intention of assisting or enabling, or being reckless as to whether the disclosure might assist or enable, any person (whether the person to whom the disclosure is made or any other person) to undertake a specified activity.[94]

4.91 For the purposes of this offence, recklessness has the following meaning:

(1) recognising a risk is created and acting;

(2) being indifferent as to whether a risk is created and acting; and

(3) acting when there is an "obvious risk" to which the person has not given thought.[95]

[89] The Atomic Energy Act 1946, s 14.

[90] The Atomic Energy Act 1946, s 14.

[91] The Atomic Energy Act 1946, s 14.

[92] Uranium Enrichment Technology (Prohibition on Disclosure) Regulations 2004/1818. Specified activities are defined in regulation 1 as: treating uranium, manufacturing enrichment equipment, adapting equipment to be enrichment equipment, and testing or evaluating enrichment equipment.

[93] Uranium Enrichment Technology (Prohibition on Disclosure) Regulations 2004/1818, reg 2.

[94] Uranium Enrichment Technology (Prohibition on Disclosure) Regulations 2004/1818, reg 2.

[95] Uranium Enrichment Technology (Prohibition on Disclosure) Regulations 2004/1818, reg 2.

4.92 This definition of recklessness is unusual. Within the criminal law, typically a person is reckless if he or she is aware of the existence of a risk and unreasonably goes on to take that risk.[96] Comparatively, there is no need to be aware of a risk in categories (2) or (3). A person who was genuinely unaware of the existence of an obvious risk or who acted without considering whether a risk existed would usually be considered to be acting negligently, not recklessly. The definition of recklessness contained in this provision therefore conflates negligence and recklessness.[97]

4.93 Exemptions from the offence are set out in regulation 3. Disclosures are exempt if: they are of relevant information made to bodies including the Office of Nuclear Information and Euratom; to allow appropriate patents and trademarks to be registered; they are allowed by an export licence; or if they have appropriate authorisation.

4.94 The method for achieving appropriate authorisation is set out in regulation 4. It requires an application to be made to the appropriate authority. The authority's response must be in writing and if they refuse they must give reasons. The applicant then has 28 days to make written applications if they want the authority to reconsider their application. The appropriate authority for applicants seeking authorisation to make a disclosure in England and Wales is the Office of Nuclear Regulation and for applicants outside the United Kingdom is the Secretary of State.[98] The maximum sentence for a section 80 disclosure is seven years' imprisonment and/or a fine.[99]

4.95 Fifthly, the Nuclear Industries Security Regulations 2003/403 create a different form of disclosure-related offence.[100] The offence is unusual because it is based on the failure to safeguard rather than on positive acts of disclosure. It can only be committed by specific people who are set out in the regulation.[101]

4.96 The regulation governing which individuals the offence applies to is complex. It applies to any person who is either in possession or control of sensitive nuclear information and undertaking a specified activity; or in possession or control of uranium enrichment technology or software and undertaking a specified activity.[102]

[96] See generally D Ormerod and K Laird, *Smith and Hogan's Criminal Law* (14th ed 2015) pp 129-139.

[97] D Ormerod and K Laird, *Smith and Hogan's Criminal Law* (14th ed 2015) pp 129-139.

[98] Uranium Enrichment Technology (Prohibition on Disclosure) Regulations 2004/1818, reg 4.

[99] Anti-terrorism, Crime and Security Act 2001, s 80.

[100] Nuclear Industries Security Regulations 2003/403, reg 22.

[101] Nuclear Industries Security Regulations 2003/403, reg 22.

[102] Nuclear Industries Security Regulations 2003/403, reg 22.

4.97 For information that relates to the nuclear industry, specified activities are those in relation to a nuclear site and uranium enrichment and related activities.[103] For uranium enrichment technology and software, specified activities are uranium enrichment and related activities.[104] The offence does not apply with regard to nuclear information if the information was neither protectively marked nor should have been.[105]

4.98 This exemption is made more complex by the fact that it contains exceptions. These exceptions mean the exemption cannot be relied upon by those working on non-nuclear premises with approved security plans, planning the development of a nuclear facility, the Nuclear Decommissioning Authority, and people related to these categories.[106] Finally, the offence does not apply to a responsible person who keeps relevant information in a place with an approved security plan.[107]

4.99 The regulation requires a person to whom it applies to maintain appropriate safety standards to minimise "the risk of…unauthorised disclosure of…any sensitive nuclear information, uranium enrichment equipment or uranium enrichment software within his possession or control". Consequently, the offence can be committed when no disclosure in fact occurs.

4.100 It is a defence for the person to show they were acting under the instruction of a person to whom the regulations apply. The maximum sentence available is two years' imprisonment and/or a fine.[108]

Information useful to an enemy

4.101 There are two national security disclosure offences related to information that might be useful to an enemy. These coexist alongside the offence contained in section 1(1)(c) of the Official Secrets Act 1911 of communicating information, for any purpose prejudicial to the safety or interests of the state, which is calculated to be or might be, or is intended to be directly or indirectly useful to an enemy. This offence is discussed fully in Chapter 2.

4.102 These additional offences are contained in the Armed Forces Act 2006 and only apply to individuals who are subject to service law.[109] Section 1 creates an offence of assisting the enemy. Under this section a person commits an offence if, without lawful excuse, he or she intentionally communicates with an enemy or gives an enemy information that would or might be useful to the enemy. The maximum sentence for this offence is life imprisonment.

[103] Nuclear Industries Security Regulations 2003/403, reg 22.

[104] Nuclear Industries Security Regulations 2003/403, reg 22.

[105] Nuclear Industries Security Regulations 2003/403, reg 22.

[106] Nuclear Industries Security Regulations 2003/403, reg 22.

[107] Nuclear Industries Security Regulations 2003/403, reg 22.

[108] Nuclear Industries Security Regulations 2003/403, reg 25. Our research has not revealed any case that has considered whether this places a burden on the defendant.

[109] Civilians can be subject to service law in a number of circumstances. See J Blackett, *Rant on the Court Martial and Service Law* (2009) ch 6.

4.103 Section 17 makes it an offence to disclose information that would or might be useful to the enemy without lawful authority. The fault element for the offence is that the discloser knows or has reasonable cause to believe that the information would or might be useful to an enemy. The maximum sentence for this offence is two years' imprisonment.

Problems with the national security disclosure offences

4.104 Given that there are fewer national security disclosure offences and they encompass distinct categories of information, the inconsistencies between these offences are not as extensive as those we examined in the previous section.

4.105 There are, however, inconsistencies between the maximum sentences available for offences that have the potential to impact upon national security, including those offences contained in the Official Secrets Acts. The maximum sentences range from two years' imprisonment to life imprisonment for the national security disclosure offences. Even if the offence of assisting the enemy contained in the Armed Forces Act 2006 is excluded, the sentence range remains unusually broad: from two years to seven years. We examine this issue with reference to the Official Secrets Acts in Chapter 3.

4.106 There are other inconsistencies between the national security disclosure offences. As Chapter 3 explained, damage is a key element of the majority of the disclosure offences contained in the Official Secrets Act 1989. Not all of the national security disclosure offences outlined in this chapter require proof of damage. Section 11 of the Atomic Energy Act 1946, for example, only requires the disclosure to be of relevant information and for the discloser to know that it falls within this category. The point here is not that the disclosures criminalised by these offences are not damaging. Rather it is that evidencing damage is not necessary to prove the offence.

4.107 The disclosure offences examined above which do require consideration of damage are not formulated in the same manner as the disclosure offences in the Official Secrets Act 1989. Section 79 of the Anti-terrorism, Crime and Security Act 2001 first requires consideration of damage as part of the conduct element of the offence. It provides that:

> A person is guilty of an offence if he discloses any information or thing the disclosure of which might prejudice the security of any nuclear site or of any nuclear material.

4.108 The section 79 offence also requires consideration of damage as part of the fault element however, as the person must either intend to or be reckless toward such damage.

4.109 There is no consistency of approach as to whether consideration of damage is necessary in national security disclosure offences. We have been unable to discern any principled reason to explain this inconsistency of approach.

Conclusion on national security disclosure offences

4.110 As our analysis of the current law has demonstrated, there are inconsistencies between the national security disclosure offences. They are perhaps explicable, however, on the basis that these offences criminalise the unauthorised disclosure of distinct and readily ascertainable sub-categories of information, in contrast to the personal information disclosure offences.

Consultation question 12

4.111 **Do consultees have a view on whether national security disclosure offences should form part of a future full review of miscellaneous unauthorised disclosure offences?**

CHAPTER 5
PROCEDURAL MATTERS RELATING TO INVESTIGATION AND TRIAL

INTRODUCTION

5.1 This chapter will examine a number of procedural matters that relate specifically to prosecutions for offences contrary to the Official Secrets Acts that we believe are worthy of detailed consideration. There are three procedural matters that we believe merit particular attention. The first is the so-called "Gateway process", which is the standard procedure adopted before any investigation for an offence contrary to the Official Secrets Acts can be initiated. The second relates to the trial and the need to ensure the continued confidentiality of any sensitive information that may have to be placed before the jury. Finally we consider the broader question of whether more extensive reform is needed of the criminal procedure that is adopted in trials that require sensitive information to be placed before a jury.

5.2 This chapter will focus only upon those disclosures that potentially engage the Official Secrets Acts. Other disclosures that do not reach that threshold may be investigated internally by investigators employed by the Government department in question.

BACKGROUND

5.3 The process for conducting investigations into potential offences under the Official Secrets Act 1989 was changed significantly as a result of a report published by Her Majesty's Chief Inspector of Constabulary in 2009.[1]

5.4 Before proceeding to analyse the circumstances that led to the report and its contents, it is necessary to describe briefly how unauthorised disclosures of information are investigated across Whitehall. Typically, if an apparent unauthorised disclosure of information is detected, it is initially investigated internally by the Government department concerned in accordance with guidance issued by the Cabinet Office.[2]

5.5 It is the Cabinet Office that has responsibility for formulating security policy standards for government and ensuring the operational delivery of this policy. In addition, the Cabinet Office provides advice and assistance to departments when an unauthorised disclosure occurs. For example, the Cabinet Office maintains a panel of approved professional investigators who can investigate unauthorised disclosures at the request of a department.

5.6 In exceptional cases, it may be considered necessary to involve the police in the investigation of an unauthorised disclosure. There is a history of the Metropolitan Police Service investigating offences under the Official Secrets Acts. More specifically, these offences are now investigated by Counter Terrorism Command

[1] Her Majesty's Inspectorate of Constabulary, *Review of the Lessons Learned from the Metropolitan Police Service's Investigation of Home Office Leaks* (2009).

[2] Cabinet Office, *Guidance on leak investigation policy and procedures* (2008).

(SO15), which has police officers who have the requisite vetting to handle sensitive information. In the context of suspected offences under the Official Secrets Act 1989, investigations are usually undertaken at the request of the Cabinet Office, however other departments may invite the police to conduct an investigation.[3] This arrangement is underpinned by a draft protocol between the Cabinet Office and SO15.[4] Although the police may be invited to conduct an investigation, it is ultimately the decision of the police whether to do so or not.

5.7 In November 2008, the Cabinet Office asked the Metropolitan Police Service to commence an investigation into a series of leaks emanating from the Home Office. Following consultation with the Crown Prosecution Service and with the approval of senior officers, investigators from Counter Terrorism Command (SO15) arrested Christopher Galley, a civil servant working in the Home Office, and Damian Green, a Member of Parliament and a Conservative Party front bench spokesperson. In April 2009, the Director of Public Prosecutions announced that no charges would be brought against either Mr Galley or Mr Green.[5]

5.8 As a result of the unusual and high profile nature of this case, a series of reviews were undertaken.[6] Following the decision of the Director of Public Prosecutions not to charge Mr Galley and Mr Green, the Home Secretary asked Her Majesty's Chief Inspector of Constabulary to review the case. The terms of reference were, "To undertake a review of the lessons learned from the Metropolitan Police investigation into Home Office leaks".[7]

5.9 The overarching conclusion of Her Majesty's Inspectorate of Constabulary was that the police should only be involved in the investigation of unauthorised disclosures of information when there is evidence that either an offence under the

[3] For example, in the context of the Ministry of Defence, the Ministry of Defence Police, the Royal Navy Police, the Royal Military Police and the Royal Air Force Police all have the capacity to investigate the suspected commission of criminal offences.

[4] Cabinet Office, *Handling unauthorised disclosures and national security cases - Protocol between Cabinet Office on behalf of Her Majesty's Government and the Metropolitan Police Counter Terrorism Command (SO15) DRAFT* (2008).

[5] Crown Prosecution Service, *Decision on prosecution - Mr Christopher Galley and Mr Damian Green MP* (16 April 2009) http://www.cps.gov.uk/news/articles/decision_on_prosecution_-_mr_christopher_galley_and_mr_damian_green_mp/ (Accessed 8 November 2016).

[6] In addition to the review undertaken by Her Majesty's Inspectorate of Constabulary, there was a review undertaken by the House of Commons Home Affairs Select Committee, *Policing Process of Home Office Leaks Enquiry*, HC 157 (2008-09). A further review was undertaken by the House of Commons Public Administration Select Committee, *Leaks and Whistleblowing in Whitehall*, Tenth Report of Session 2008-09, 16 July 2009. Following the case, a review was also undertaken to examine the issue of privilege relating to police searches by the Parliamentary Committee on the issue of privilege, *Police searches on the Parliamentary Estate. Committee on Issue of Privilege first report with formal minutes, evidence*, HC 62 (2009-10).

[7] Her Majesty's Inspectorate of Constabulary, *Review of the Lessons Learned from the Metropolitan Police Service's Investigation of Home Office Leaks* (2009) para 4.7.

Official Secrets Act 1989 or some other serious criminal offence has been committed.[8]

5.10 Her Majesty's Inspectorate of Constabulary recommended the creation of a protocol to inform the police and other stakeholders of the criteria for involving the police in future investigations. The report elaborated as follows:

> The aim of the protocol is to develop a staged process between the police, the Crown Prosecution Service, Cabinet Office and a designated Parliamentary official to deal with investigations of this nature. The Protocol describes a process which encourages key stakeholders to contribute to the decision making, whilst recognising the independence of each organisation.[9]

5.11 The aim was for this protocol to be versatile, so that it could be applied more widely to other allegations of serious crimes involving Parliament, Members of Parliament and officials. To this end, the Protocol was to apply irrespective of whether the alleged criminal offence was committed by a Member of Parliament.

5.12 This protocol was annexed to the report produced by Her Majesty's Chief Inspector of Constabulary. The protocol sets out a 7 step process for investigating leaks. The report made clear that there should be a presumption in favour of the police *not* being involved unless there are reasonable grounds for believing that the following criteria are satisfied:

(1) Reasonable grounds for believing an offence under the Official Secrets Act 1989 has been committed.

(2) Reasonable grounds for believing a serious criminal offence has been committed, such as bribery or corruption, or very exceptional cases which seriously threaten the United Kingdom in economic or integrity terms.[10]

5.13 The Report also stated that if a Member of Parliament is suspected of an offence, the impact of parliamentary privilege must be addressed and constantly assessed during the investigation.[11]

5.14 We have reproduced the 7 step process recommended by Her Majesty's Chief Inspector of Constabulary on the following two pages. In its response to the Public Administration Select Committee's Report entitled "Leaks and Whistleblowing in Whitehall", the Government confirmed that the protocol has

[8] Her Majesty's Inspectorate of Constabulary, *Review of the Lessons Learned from the Metropolitan Police Service's Investigation of Home Office Leaks* (2009) para 9.3.

[9] Her Majesty's Inspectorate of Constabulary, *Review of the Lessons Learned from the Metropolitan Police Service's Investigation of Home Office Leaks* (2009) para 9.4.

[10] Her Majesty's Inspectorate of Constabulary, *Review of the Lessons Learned from the Metropolitan Police Service's Investigation of Home Office Leaks* (2009) p 61.

[11] Her Majesty's Inspectorate of Constabulary, *Review of the Lessons Learned from the Metropolitan Police Service's Investigation of Home Office Leaks* (2009) p 61.

been adopted.[12] In this document, the Government emphasised that the Cabinet Office, given that it has overall responsibility for the Government's security policy framework, must be consulted in any consideration of whether to refer an unauthorised disclosure to the police, to ensure that all decisions are consistent with this protocol.

THE PROTOCOL

Step One – Internal investigation

It is the responsibility of Government Departments to ensure they have a security regime in place which: is fit for purpose; prevents leaks; encompasses whistle blowing; and fosters a culture of integrity regarding disclosure of information. Leaks should be investigated by suitably experienced internal investigators capable of exploiting investigative opportunities, with analytical support when appropriate. Before referral to the Cabinet Office, Departments should be able to present a clear intelligence/evidence based package, meeting the threshold required to instigate police involvement.

Step Two – Meeting the threshold for police involvement

The threshold for police involvement is high. Only in leak cases where the Cabinet Office believes there is intelligence/evidence to suggest the criteria of Official Secrets Act criminality has been reached or in leak cases where the criteria has not been reached but there are compelling grounds to suspect a serious offence (as described in the introduction) has been committed should a case be presented to the Gateway process. Before moving to the Gateway stage, consideration should be given to the proportionality of police involvement, likely outcomes and other internal resolution options.

Step Three – The Gateway process

The Gateway can be accessed only through nominated Single Points of Contact (SPOCs). These SPOCs should occupy senior executive positions within the Cabinet Office and other relevant participant organisations. In the case of the MPS the level has been suggested at Deputy Commissioner. The Director of Public Prosecutions and Commissioner of the MPS have agreed to high level Gateway representation as a useful development. Other representatives may be invited to attend as appropriate. The panel of SPOCs will assess the strength of the intelligence/evidence package and decide whether it meets the threshold for police investigation. At this early stage the panel should consider likely outcomes and other resolution options, for example using appropriate regulatory authorities; whether an investigation represents the best use of police resources; and if it is in the public interest to investigate. The panel might also require further scoping of the case to take place before deciding upon the next step. Each organisation represented clearly has its own responsibilities and

[12] Government response to the tenth report of session 2008 to 2009 from the Public

independence in this process; the objective is to see if collective agreement can be secured on the value of going forward. It is also understood, that at any stage, each of these organisations can exercise their individual independence as necessary given their different roles. Notwithstanding this principle, in extraordinary circumstances it may be necessary for the police to act outside these guidelines and not to fetter their independence by doing so. These situations would be exceptional and require a transparent rationale for taking such action.

Step four – Scoping

The Gateway Panel may request further work to assist in their considerations of the most appropriate course of action. This may be undertaken by the Cabinet Office/ Department or jointly with the police if they are able to bring added value to the process. If the police are engaged it should be clearly understood that this is not the start of an investigation, which should only commence once agreed by the Gateway Panel. Whilst undertaking the scoping, cognisance should be taken of the criteria applied in the Gateway.

Step five – Police investigation

Once an investigation has commenced, progress should be regularly reviewed against all resolution options including ceasing to investigate. In common with national best practice derived from other high risk cases, police will establish an early relationship with a senior level Crown Prosecution Service lawyer and take advice at key stages of the investigation. When the investigation has Parliamentary implications, seeking advice from a Parliamentary official at an appropriate stage of the investigation would be advisable. Both these relationships should be separate to any formal police review process.

Step six – Regular review

This should be an ongoing process involving the Police, Crown Prosecution Service and any other representative adding value. It is suggested that the introduction of someone not forming part of the investigation command team, who can independently challenge decision making, would be an asset to the quality of decision making. The purpose of the review is to take stock of the investigation. By considering the likely outcomes, resolution options and other relevant factors, the review will be capable of deciding the most appropriate course of action. In doing so, levels of actual harm or damage as revealed by the investigation will inform the police/CPS decisions as to public interest.

Step seven – Resolution options

Administration Select Committee (2010) Cm 7863 para 13.

> At the conclusion of the investigation – assuming it has passed through the review process – there will be a determination of how the case will be concluded. The Director of Public Prosecutions will first decide whether any criminal proceedings should be pursued. In the event of there being no proceedings, other resolution options should be considered.

The extent to which improvements can be made

5.15 This section will examine in greater detail and assess whether the Protocol could be improved. What is immediately obvious is that the Protocol mandates a very different investigative process than would ordinarily apply. This is because it is unusual for a Government department to play such a central role in the assessment of whether a criminal offence has been committed and whether the police ought to be invited to investigate a possible criminal offence. The Protocol does make clear, however, that the independence of the police from the Executive must be maintained. This is a fundamental principle that was enunciated by Lord Denning in *Blackburn* in the following terms:

> I have no hesitation in holding that, like every constable in the land, the [Commissioner of the Metropolitan Police] should be, and is, independent of the executive.[13]

5.16 The Protocol reinforces this principle by stipulating that once the decision is taken to initiate a police investigation, then it must be free of any executive influence. In addition, the Protocol states that the police ought to establish an early relationship with a senior lawyer within the Crown Prosecution Service who can provide advice at key stages in the investigative process.

5.17 Despite the existence of these safeguards, our initial consultation with stakeholders has led us provisionally to conclude that there are ways in which the Protocol could be improved. These are mainly attributable to the fact the Protocol was reactive and drafted in response to a specific incident yet it applies to all instances of unauthorised disclosure. For these reasons, it should not be surprising that after a number of years' use the Protocol could be subject to refinement.

The multifaceted nature of the process

5.18 We believe that the Protocol, and the Gateway process in particular, fulfils a number of different functions, which we list below:

(1) Coordinating the attempt to identify the source of the unauthorised disclosure, with a view to that person potentially being charged with a criminal offence.

(2) Maintaining consistency of approach as to how unauthorised disclosures are handled across government.

[13] *R v Commissioner of Police of the Metropolis ex parte Blackburn (No 1)* [1968] 2 QB 118, 135, by Lord Denning MR.

(3) Ensuring that if a serious criminal offence is alleged to have been committed by a Parliamentarian, then appropriate measures can be taken to ensure the investigative process accounts for the sensitivity of such an allegation.

(4) Serving to filter less serious allegations. Not every unauthorised disclosure constitutes a criminal offence, so the Protocol ensures that the police are not invited to investigate disclosures that do not cross the high threshold into criminal liability. Such disclosures can be dealt with adequately by internal disciplinary measures including dismissal.

(5) The involvement of Counter Terrorism Command in an investigation is costly and should not be undertaken lightly, so the Protocol ensures sufficient thought can be given as to the proportionality of initiating such an investigation.

(6) Given the availability of disciplinary sanctions rather than a criminal offence, the Protocol ensures that sufficient consideration is given to whether the former is a more proportionate response to the unauthorised disclosure.

(7) If information has been disclosed that could jeopardise national security, the Protocol ensures that steps can be taken to retrieve the information as quickly as possible with the aim of minimising the chance that national security will be jeopardised.

5.19 We believe there is the potential for these different functions to conflict. For example, in seeking to ensure that sensitive information is retrieved and secured as quickly as possible so as to minimise the risk to national security, there is the risk that evidence may be contaminated. This may undermine the ability to prosecute the individual who disclosed the information.

Provisional conclusion 18

5.20 **We provisionally conclude that improvements could be made to the Protocol. Do consultees agree?**

Options for reform

5.21 There is no doubt that the Protocol fulfils an important function. We do believe, however, that improvements could be made. These would ensure that the system would lead to the police being invited to investigate disclosures only where they cross the threshold into serious criminality, whilst minimising the potential contamination of evidence. It is also necessary to ensure the process is as transparent as possible and that it maintains a consistency of approach.

The meaning of "serious offence"

5.22 The first improvement we believe could be made is for greater clarity in the Protocol as to the types of criminal offence to which it applies. The Protocol states that a case should only be presented to the Gateway if there is evidence that an offence contrary to the Official Secrets Acts has been committed or there are compelling grounds to believe some other "serious offence" has been

committed.[14] The Protocol does not, however, specify what is meant by "serious offence" in this context. There is the possibility that this term could be misconstrued. We therefore believe there is merit in considering what types of serious criminal offence require a procedure such as the one mandated by the Protocol. For example, arguably it should only be those serious criminal offences where the conduct has implications for national security that should engage the Protocol.

Earlier legal involvement

5.23 The second improvement is to ensure that the process evidences a clear commitment to legal outcomes in addition to supressing the risk of further damage. To achieve this, one option is to have greater legal involvement earlier in the process from the Crown Prosecution Service, for example. This would ensure that the risk of the information being further disseminated is minimised, whilst maximising the potential for any evidence subsequently to be admissible in a criminal trial. This would also ensure that other offences that may have been committed can be identified. As we have already discussed, however, one of the reasons the Protocol exists is to ensure sensitive information can be retrieved quickly. A decision could be taken to maximise the possibility of retrieving the information quickly, knowing that this might undermine the ability to bring a prosecution. In circumstances where there is a tension between retrieving the information and being able to commence a prosecution, a decision could be taken to prefer the former.

Consultation question 13

5.24 **Do consultees have a view on whether defining the term "serious offence" and ensuring earlier legal involvement would make the Protocol more effective?**

Consultation question 14

5.25 **Do consultees have views on how the Protocol could be improved?**

THE TRIAL PROCESS

5.26 This section will examine the issues that can arise when an individual is prosecuted for an offence contrary to the Official Secrets Acts, with an emphasis upon those that relate to the conduct of the trial. These are attributable to the fact that a trial for an Official Secrets Act offence will involve information that potentially relates to national security and is therefore of an extremely sensitive nature. This section will examine the following issues:

(1) Excluding members of the public from the court.

(2) Jury vetting/checks.

(3) Common issues that apply to criminal trials in which sensitive information may be disclosed more generally.

[14] Her Majesty's Inspectorate of Constabulary, *Review of the Lessons Learned from the Metropolitan Police Service's Investigation of Home Office Leaks* (2009) p 61.

The ability to exclude members of the public from the court during the proceedings

5.27 It has long been recognised that the principle of open justice is fundamental to the rule of law and democratic accountability. In *Scott v Scott*, Lord Shaw of Dunfermline described publicity in the administration of justice as "one of the surest guarantees of our liberties".[15] In more recent times, this principle was expounded by Lord Diplock in *Attorney General v Leveller Magazine Ltd* in the following terms:

> If the way that courts behave cannot be hidden from the public ear and eye this provides a safeguard against judicial arbitrariness or idiosyncrasy and maintains the public confidence in the administration of justice. The application of this principle of open justice has two aspects: as respects proceedings in the court itself it requires that they should be held in open court to which the press and public are admitted and that, in criminal cases at any rate, all evidence communicated to the court is communicated publicly. As respects the publication to a wider public of fair and accurate reports of proceedings that have taken place in court the principle requires that nothing should be done to discourage this.[16]

5.28 In this case Lord Diplock did recognise, however, that this principle is not absolute and may be subject to exceptions:

> However, since the purpose of the general rule is to serve the ends of justice it may be necessary to depart from it where the nature or circumstances of the particular proceeding are such that the application of the general rule in its entirety would frustrate or render impracticable the administration of justice or would damage some other public interest for whose protection Parliament has made some statutory derogation from the rule. Apart from statutory exceptions, however, where a court in the exercise of its inherent power to control the conduct of proceedings before it departs in any way from the general rule, the departure is justified to the extent and to no more than the extent that the court reasonably believes it to be necessary in order to serve the ends of justice.[17]

5.29 In *Scott v Scott* Viscount Haldane LC stated that a court must not exercise its power to exclude the public unless it is demonstrated to be "strictly necessary" and "that by nothing short of the exclusion of the public can justice be done".[18]

5.30 In the context of a prosecution for an offence contrary to the Official Secrets Acts, section 8(4) of the Official Secrets Act 1920 provides:

> Without prejudice to any powers which a court may possess to order the exclusion of the public from any proceedings if, in the course of

[15] *Scott v Scott* [1913] AC 417, 476, by Lord Shaw of Dunfermline.

[16] *Attorney General v Leveller Magazine Ltd* [1979] AC 440, 450, by Lord Diplock.

[17] *Attorney General v Leveller Magazine Ltd* [1979] AC 440, 450, by Lord Diplock.

[18] *Scott v Scott* [1913] AC 417, 438, by Viscount Haldane LC.

> proceedings before a court against any person for an offence under the principal Act or this Act or the proceedings on appeal, or in the course of the trial of a person for felony or misdemeanour under the principal Act or this Act, application is made by the prosecution, on the ground that the publication of any evidence to be given or of any statement to be made in the course of the proceedings would be prejudicial to the national safety, that all or any portion of the public shall be excluded during any part of the hearing, the court may make an order to that effect, but the passing of sentence shall in any case take place in public.

5.31 The Official Secrets Act 1920 therefore constitutes a statutory exception to the principle of open justice.[19] By virtue of section 12(1)(c) of the Administration of Justice Act 1960, publication of information relating to proceedings that are held in private for reasons relating to national security constitutes a contempt of court.

5.32 Section 8(4) of the Official Secrets Act 1920 gives the court the power to exclude the public from trials when publication of any evidence would be "prejudicial to the national safety". This statutory power sits alongside the common law powers of the courts to hear trials in private. In *Attorney General v Leveller Magazine*, Lord Scarman gave the following explanation for why it was considered necessary to adopt section 8(4):

> Parliament deemed it necessary to augment in the Official Secrets cases, whatever common law powers a court had to sit in private by one the exercise of which would not be dependent upon the court's assessment of the danger of publicity to the administration of justice.[20]

5.33 In the recent case of *Guardian News and Media Ltd v R & Erol Incedal* Lord Thomas of Cwmgiedd CJ took the opportunity to restate the applicable principles that apply when the prosecution is considering making an application for a case to be heard in private. This was not a prosecution for an offence contrary to the Official Secrets Acts. Therefore the Court of Appeal was discussing this issue in the context of the courts' common law powers. We believe, however, that these principles are also relevant in the context of the power contained in section 8(4) of the Official Secrets Act 1920:

(1) It is for the Director of Public Prosecutions to decide whether to apply to the court for part of the proceedings to be held in private. This is a matter solely for the Director of Public Prosecutions, subject to the superintendence of the Attorney General and in exceptional cases the court by way of judicial review. After the court decides whether to grant the Director of Public Prosecution's request, it is for her to decide

[19] The procedure for applying for a trial or part of a trial to be heard in private is contained in *Criminal Procedure Rules* (2016), rules 6.6 – 6.7. For discussion, see D Ormerod and D Perry, *Blackstone's Criminal Practice* (2017), at D3.122 – D3.134.

[20] *Attorney General v Leveller Magazine* [1979] AC 440, 470. See also M L Friedland, *National Security: The Legal Dimension* (1979) p 46.

whether to continue the prosecution, taking into account the interests of national security when necessary.[21]

(2) When the Director of Public Prosecution makes the application to the court, the court must proceed on the basis that the principle of open justice is fundamental to the rule of law and to democratic accountability. It is for the Director of Public Prosecutions to make a very clear case.[22] He elaborated in the following terms:

> Thus in each case, it is for the court to determine on this very strict test whether the detailed reasons that have been put forward in the particular circumstances for departing from the general principle of open justice as regards particular matters or evidence in the course of proceedings necessitate a departure from the fundamental principle of open justice.[23]

(3) Where the reason for departing from the principle of open justice is based on reasons relating to national security, it is for the court and the court alone to determine if the stringent test has been met. It must decide whether the evidence or material in question should be heard in public or not. The reasons will often be contained in a certificate submitted to the court by the Director of Public Prosecutions on behalf of the Secretary of State.[24] In relation to the weight the court ought to give to that certificate, the Lord Chief Justice stated:

> In making that decision the court will pay the highest regard to what is stated by the Secretary of State in his or her Certificate. As Lord Hoffman made clear in *Secretary of State for the Home Department v Rehman* [2003] 1 AC 153, paras 50–57, a court should not depart from the view of the Secretary of State on national security issues, provided there is an evidential basis for the decision of the Secretary of State. That is because under our constitution the identification and delineation of national security interests is for the Executive branch of the state. Although the circumstances will be very rare, the court is also free to depart from the views set out in the Certificate as to the weight to be attached to the national security interests. That is because it is always for the court to make the decision on

[21] *Guardian News and Media Ltd v R & Erol Incedal* [2016] EWCA Crim 11 at [43] – [46], by Lord Thomas of Cwmgiedd CJ.

[22] *Guardian News and Media Ltd v R & Erol Incedal* [2016] EWCA Crim 11 at [47] – [49], by Lord Thomas of Cwmgiedd CJ.

[23] *Guardian News and Media Ltd v R & Erol Incedal* [2016] EWCA Crim 11 at [50], by Lord Thomas of Cwmgiedd CJ.

[24] *Guardian News and Media Ltd v R & Erol Incedal* [2016] EWCA Crim 11 at [51] – [52], by Lord Thomas of Cwmgiedd CJ.

> whether those interests necessitate the departure from the principle of open justice.[25]

5.34 The Lord Chief Justice made clear that the question of whether to hold part of the hearings in private is a matter for the court and not the Director of Public Prosecutions. This was characterised as being a constitutional principle. He emphasised that the proper approach is for the court to examine the nature of the evidence and to determine the effect of hearing it in public. It was held that deciding whether to depart from the principle of open justice on the basis that the Director of Public Prosecutions might not continue with the prosecution if evidence is heard in open court does not satisfy the test of necessity. The reason given for this was that, in effect, it would transfer the decision on whether to depart from the principle of open justice from the court to the Director of Public Prosecutions.[26]

5.35 This decision reaffirms the general principles of open justice and their continued applicability in the modern trial. The court has not, however, addressed the specific statutory context of a trial for an offence contrary to the Official Secrets Acts.

5.36 It is unclear whether the exercise of the power conferred upon the court by section 8(4) of the Official Secrets Act 1920 is subject to the necessity test enunciated in *Scott v Scott* and affirmed more recently in *Guardian News and Media Ltd v R & Erol Incedal.* There is authority to suggest that this test does not apply. For example in the judgment of the Divisional Court in *Attorney General v Leveller Magazine Ltd*, Lord Widgery CJ stated:

> It is argued that if reliance is placed on section 8 (4) of the Official Secrets Act 1920, the Crown must provide sworn evidence that disclosure would "be prejudicial to the national safety." We cannot accept this. Courts should of course always be alert to the importance of keeping proceedings before the public and should examine with care the argument in favour of secrecy, but it will often happen that something less than formal proof is all that is available.[27]

5.37 Although the point was not addressed directly when the case came before the House of Lords, Lord Diplock did make the following observation:

> In the instant case the magistrates would have had power to sit in camera to hear the whole or part of the evidence of 'Colonel B' if this had been requested by the prosecution; and although they would not have been bound to accede to such a request it would naturally and properly have carried great weight with them. So would the absence of any such request. Without it the magistrates, in my opinion, would have had no reasonable ground for believing that so drastic a derogation from the general principle of open justice as is involved in

[25] *Guardian News and Media Ltd v R & Erol Incedal* [2016] EWCA Crim 11 at [52], by Lord Thomas of Cwmgiedd CJ.

[26] *Guardian News and Media Ltd v R & Erol Incedal* [2016] EWCA Crim 11 at [53], by Lord Thomas of Cwmgiedd CJ.

[27] *Attorney General v Leveller Magazine Ltd* [1978] QB 31, 44-45, by Lord Widgery CJ.

> hearing evidence in a criminal case in camera was necessary in the interests of the due administration of justice.[28]

5.38 In this paragraph Lord Diplock seems to be envisaging the application of a necessity test, which stands in contrast to the approach adopted earlier by Lord Widgery CJ. Given the fundamental nature of the principle of open justice, we believe that the exercise of this power should be made subject to the test of necessity and that ideally this should be made explicit within a reformed statute.

5.39 This would have two benefits. First, it would ensure that the fundamental nature of the principle of open justice is more accurately reflected in statute. Secondly, it would ensure that the power conferred upon the court by section 8(4) of the Official Secrets Act 1920 is aligned with the applicable common law rule.

5.40 In addition to its ability to order the public to be excluded from the proceedings, the court has additional powers that impact upon the principle of open justice contained in statutes other than the Official Secrets Acts. Section 4(2) of the Contempt of Court Act 1981 makes provision for the postponement of reports of legal proceedings held in public. This power may only be exercised if it appears to the court that there is a substantial risk of prejudice to the administration of justice. In addition, section 11 of the Contempt of Court Act 1981 gives the court the power to prohibit the publication of matters exempted from disclosure in open court.[29] For example, if the name of a witness was withheld from the public, then the court can give directions prohibiting the publication of that name. These powers supplement those contained in the Official Secrets Act 1920. In *Guardian News and Media Ltd v R & Erol Incedal* the Lord Chief Justice stated that the Intelligence and Security Committee of Parliament can ensure matters are properly scrutinised in cases such as these, where there is the absence of media scrutiny.[30]

Provisional conclusion 19

5.41 **The power conferred on the court by section 8(4) of the Official Secrets Act 1920 ought to be made subject to a necessity test whereby members of the public can only be excluded if necessary to ensure national safety (the term used in the 1920 Act) is not prejudiced. Do consultees agree?**

Jury checks

5.42 Section 118 of the Criminal Justice Act 1988 abolished the right of the defence to challenge jurors without cause.[31] The prosecution right to do so was, however, retained. This means that the prosecution can object to a potential juror without giving any reason. This is an exceptional power and, in recognition of this, the Attorney General periodically issues guidance to prosecutors on its use.

[28] *Attorney General v Leveller Magazine Ltd* [1979] AC 440, 451, by Lord Diplock.

[29] For discussion see *Reporting restrictions guide* (2015). Available at: https://www.judiciary.gov.uk/wp-content/uploads/2015/05/reporting-restrictions-guide-2015-final.pdf (last visited 8 November 2016).

[30] *Guardian News and Media Ltd v R & Erol Incedal* [2016] EWCA Crim 11 at [75], by Lord Thomas of Cwmgiedd CJ.

[31] J Gobert, "The peremptory challenge - an obituary" [1989] *Criminal Law Review* 528.

5.43 Use of the right of "stand by", as it is known, is limited to those cases which involve national security or terrorism.[32] The guidelines issued by the Attorney General outline the circumstances in which it is appropriate for the prosecution to exercise this power and the procedure which is to be followed.[33] The guidelines make clear that the authority to use this power must be personally authorised by the Attorney General, on the application of the Director of Public Prosecutions. The most recent guidelines are reproduced below:[34]

> 1. The principles which are generally to be observed are:
>
> > a. that members of a jury should be selected at random from the panel,
> >
> > b. the Juries Act 1974 identifies those classes of persons who alone are either disqualified from or ineligible for service on a jury; no other class of person may be treated as disqualified or ineligible,
> >
> > c. the correct way for the Crown to seek to exclude a member of the panel from sitting as a juror is by the exercise in open court of the right to request a stand by or, if necessary, to challenge for cause.
>
> 2. Parliament has provided safeguards against jurors who may be corrupt or biased. In addition to the provision for majority verdicts, there is the sanction of a criminal offence for a disqualified person to serve on a jury. The omission of a disqualified person from the panel is a matter for court officials - they will check criminal records for the purpose of ascertaining whether or not a potential juror is a disqualified person.
>
> 3. There are, however, certain exceptional types of case of public importance for which the provisions as to majority verdicts and the disqualification of jurors may not be sufficient to ensure the proper administration of justice. In such cases it is in the interests of both justice and the public that there should be further safeguards against the possibility of bias and in such cases checks which go beyond the investigation of criminal records may be necessary.
>
> 4. These classes of case may be defined broadly as (a) cases in which national security is involved and part of the evidence is likely to be heard in camera, and (b) security and terrorist cases in which a juror's extreme beliefs could prevent a fair trial.

[32] Governed by *Criminal Procedure Rules* (2016), rule 25.8(3). Discussed in D Ormerod and D Perry (eds), *Blackstone's Criminal Practice* (2017), at D13.22 – D13.45.

[33] For early analysis, see A Nicol, "Official Secrets and Jury Vetting" [1978] *Criminal Law Review* 284.

[34] *Attorney General's Guidelines (Juries: Right to Stand By)* (1989) 88 Cr App R 123. Discussed in D Ormerod and D Perry (eds), *Blackstone's Criminal Practice* (2017), at D13.45.

5. The particular aspects of these cases which may make it desirable to seek extra precautions are:

a. in security cases a danger that a juror, either voluntarily or under pressure, may make an improper use of evidence which, because of its sensitivity, has been given in camera,

b. in both security and terrorist cases the danger that a juror's personal beliefs are so biased as to go beyond normally reflecting the broad spectrum of views and interests in the community to reflect the extreme views of sectarian interest or pressure group to a degree which might interfere with his fair assessment of the facts of the case or lead him to exert improper pressure on his fellow jurors.

6. In order to ascertain whether in exceptional circumstances of the above nature either of these factors might seriously influence a potential juror's impartial performance of his duties or his respecting the secrecy of evidence given in camera, it may be necessary to conduct a limited investigation of the panel. In general, such further investigation beyond one of criminal records made for disqualifications may only be made with the records of the police. However, a check may, additionally be made against the records of the Security Service. No checks other than on these sources and no general inquiries are to be made save to the limited extent that they may be needed to confirm the identity of a juror about whom the initial check has raised serious doubts.

7. No further investigation, as described in para.6 above, should be made save with the personal authority of the Attorney General on the application of the Director of Public Prosecutions and such checks are hereafter referred to as 'authorised checks'. When a chief officer of police or the prosecutor has reason to believe that it is likely that an authorised check may be desirable and proper in accordance with these guidelines, he should refer the matter to the Director of Public Prosecutions. In those cases in which the Director of Public Prosecutions believes authorised checks are both proportionate and necessary, the Director will make an application to the Attorney General.

8. The Director of Public Prosecutions will provide the Attorney General with all relevant information in support of the requested authorised checks. The Attorney General will consider personally the request and, if appropriate, authorise the check.

9. The result of any authorised check will be sent to the Director of Public Prosecutions. The Director will then decide, having regard to the matters set out in para.5 above, what information ought to be brought to the attention of prosecuting counsel. The Director will also provide the Attorney General with the result of the authorised check.

10. Although the right of stand by and the decision to authorise checks are wholly within the discretion of the Attorney General, when

the Attorney General has agreed to an authorised check being conducted, the Director of Public Prosecutions will write to the Presiding Judge for the area to advise him that this is being done.

11. No right of stand by should be exercised by counsel for the Crown on the basis of information obtained as a result of an authorised check save with the personal authority of the Attorney General and unless the information is such as, having regard to the facts of the case and the offences charged, to afford strong reason for believing that a particular juror might be a security risk, be susceptible to improper approaches or be influenced in arriving at a verdict for the reasons given above.

12. Information revealed in the course of an authorised check must be considered in line with the normal rules on disclosure.

13. A record is to be kept by the Director of Public Prosecutions of the use made by counsel of the information passed to him and of the jurors stood by or challenged by the parties to the proceedings. A copy of this record is to be forwarded to the Attorney General for the sole purpose of enabling him to monitor the operation of these guidelines.

14. No use of the information obtained as a result of an authorised check is to be made except as may be necessary in direct relation to or arising out of the trial for which the check was authorised. The information may, however, be used for the prevention of crime or as evidence in a future criminal prosecution, save that material obtained from the Security Service may only be used in those circumstances with the authority of the Security Service.

5.44 The guidance issued by the Crown Prosecution Service on authorised jury checks suggests that the request by the Director of Public Prosecutions to the Attorney General for an authorised jury check should, if at all possible, accompany the papers requesting the consent to proceedings.

5.45 Given that the Official Secrets Acts relate to national security, it is safe to assume that it may be necessary to undertake an authorised jury check in some cases.

5.46 Given the nature of cases involving terrorism and cases that touch upon national security, we believe this process continues to fulfil an important role in the context of the Official Secrets Acts. In addition, our initial consultation with stakeholders has not suggested that this process gives rise to problems in practice. Admittedly this is difficult to assess given the fact that prosecutions for offences contrary to the Official Secrets Acts are so rare. We do, however, believe the guidance ought to be amended by making clear that if authorised jury checks have been undertaken, that this is brought to the attention of the defence.

5.47 It is important that the defendant in the case and the public at large are confident that the jury in any trial remains randomly selected. Transparency in any process that may be perceived to be an infringement of the random selection principle is vital.

Provisional conclusion 20

5.48 **The guidance on authorised jury checks ought to be amended to state that if an authorised jury check has been undertaken, then this must be brought to the attention of the defence representatives. Do consultees agree?**

Issues that apply more generally to criminal trials in which sensitive information may be disclosed

5.49 The previous sections have examined narrow issues that may arise in the context of a trial involving the Official Secrets Acts. These issues could, however, arise in the context of any criminal trial that involves the disclosure of information that relates to national security.

5.50 As we have already discussed the court has a common law power to order the trial, or sections of the trial, to be heard in private if necessary to ensure the administration of justice is not prejudiced. In a prosecution for an offence contrary to the Official Secrets Acts, this common law power is augmented by section 8(4) of the Official Secrets Act 1920.

5.51 In addition, section 4(2) of the Contempt of Court Act 1981 empowers the court to order that the publication of any report of the proceedings of a case, or part of a case, be postponed if necessary to avoid a substantial risk to the administration of justice. By virtue of section 11 of the Contempt of Court Act 1981, where a court allows a name or other matter to be withheld from the public, the court may give such directions prohibiting the publication of that name or matter as appear to the court to be necessary for the purpose for which it was so withheld.

5.52 In the context of the civil law, a systematic review of the relevant procedures has been undertaken with the aim of striking a balance between the imperative to ensure national security and the administration of justice are not jeopardised with ensuring the right to a fair trial and upholding the principle of open justice.

5.53 In this section we briefly describe these changes, without commenting upon whether they manage successfully to reconcile the two imperatives outlined in the previous paragraph.[35] Our aim is not to suggest that the procedure that is applicable in the civil context ought to be imported wholesale into the criminal. Rather, we are seeking to highlight the fact that the criminal trial has received relatively little attention when compared with the civil trial.

5.54 Part 2 of the Justice and Security Act 2013 provides for what is called "Closed Material Procedure" which permits courts to consider any material the disclosure of which would be "damaging to the interests of national security" without such

[35] For a general discussion of the effort to reconcile national security with the right to a fair trial in the civil context see D Heaton, "Carnduff, Al Rawi, the "unfairness" of public interest immunity and sharp procedure" 34(2) (2015) *Civil Justice Quarterly* 191; J Jackson, "Justice, Security and the right to a fair trial: is the use of secret evidence ever fair?" (2013) *Public Law* 720; Joint Committee on Human Rights, *Counter-Terrorism Policy and Human Rights: 28 days, intercept and post-charge questioning*, Nineteenth Report of Session 2006-07.

material being disclosed to the non-Governmental party to the case.[36] The court, on the application of the Secretary of State or any party to the proceedings, may make a declaration that material can be withheld from the non-Governmental party to the case.

5.55 Before it can do so, the court must be satisfied that a party to the proceedings would be required to disclose sensitive material in the course of the proceedings to another person and that it is in the interests of fair and effective administration of justice in the proceedings to make such a declaration.

5.56 In proceedings such as these, a special advocate may be appointed to represent the interests of a party in closed material proceedings.[37]

5.57 These amendments to the law were enacted as a result of the Justice and Security Green Paper that was published in October 2011,[38] with the specific aim of reconciling the rights enshrined in Article 6 of the European Convention on Human Rights with the need to protect sensitive sources, capabilities and techniques and the United Kingdom's relationship with international partners.

5.58 There are a number of other Acts that make specific provision for closed material proceedings. For example, such provision is contained in both the Special Immigration Appeals Commission Act 1997 and the Terrorism Prevention and Investigation Measures Act 2011. These differ from the powers contained in the Justice and Security Act 2013, because they give the court the power to order that material be withheld if disclosure would be contrary to the public interest.

5.59 In contrast to the civil law, the criminal law still relies upon the common law and legislation not necessarily drafted with the aim of reconciling these competing interests. The fact there has been no systematic review perhaps explains why the common law test for when it is justified to depart from the principle of open justice refers to the need to ensure the administration of justice is not prejudiced, whilst the test in section 8(4) of the Official Secrets Act 1920 refers to the need to ensure the national safety is not prejudiced.[39] Although not strictly within our terms of reference, we have provisionally concluded it is necessary to undertake a separate review to consider whether there are improvements that could be made to the current system. This would provide the opportunity to tailor these powers with the specific aim of reconciling national security imperatives with the right to a fair trial and the principle of open justice.

Provisional conclusion 21

5.60 **A separate review ought to be undertaken to evaluate the extent to which the current mechanisms that are relied upon strike the correct balance**

[36] For discussion, see C Walker, "Living with national security disputes in court in England and Wales" in G Martin, R Scott Bray and M Kumar (eds), *Secrecy, Law and Society* (2015) pp 23-43.

[37] In the criminal context special counsel may be used. For discussion, see J Jackson, "The role of special advocates: advocacy, due process and the adversarial tradition" 20(4) (2016) *International Journal of Evidence and Proof* 343.

[38] Justice and security green paper (2011) Cm 8194.

[39] The extent to which these two tests differ as a matter of substance is debatable.

between the right to a fair trial and the need to safeguard sensitive material in criminal proceedings. Do consultees agree?

CHAPTER 6
FREEDOM OF EXPRESSION

INTRODUCTION

6.1 In this chapter, we consider the extent to which offences that criminalise the unauthorised disclosure of information impact upon the right to freedom of expression. As we have discussed in other chapters, it is not just the right to freedom of expression that the provisions analysed in this paper impact upon. We believe it is appropriate to devote a single chapter to the impact on freedom of expression, however, due to the fact that this is the right most consistently implicated in the provisions we are considering.

6.2 Since at least the Enlightenment, freedom of expression has been recognised as being fundamental to democracy.[1] In the modern era, the importance of freedom of expression is reflected by its inclusion in every international human rights instrument. For example, article 19 of the Universal Declaration on Human Rights provides:

> Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.[2]

6.3 In the domestic law context, the right to freedom of expression has been recognised as being fundamental on numerous occasions. For example, In *Shayler* Lord Bingham stated:

> Modern democratic government means government of the people by the people for the people. But there can be no government by the people if they are ignorant of the issues to be resolved, the arguments for and against different solutions and the facts underlying those arguments.[3]

6.4 In *Reynolds v Times Newspapers Limited* Lord Steyn stated that freedom of expression is guaranteed in domestic law by three mechanisms:

(1) The principle of liberty, which means that individuals are free to do whatever is not specifically prohibited by law.

(2) The constitutional right to freedom of expression enshrined in the common law. It was held that, "by categorising this basic and fundamental right as a constitutional right its higher normative force is emphasised".[4]

[1] For extensive discussion, see E Barendt, *Freedom of Speech* (2nd ed 2007) ch 1.

[2] The United Nations, *The Universal Declaration on Human Rights* (1948).

[3] *R v Shayler* [2002] UKHL 11, [2003] 1 AC 247 at [21].

[4] *Reynolds v Times Newspapers Ltd and Others* [2001] 2 AC 127, 207, by Lord Steyn.

(3) Article 10 of the European Convention on Human Rights, which was incorporated into domestic law by the Human Rights Act 1998.[5]

6.5 Given its status as a constitutional right, freedom of expression was protected in domestic law long before article 10 of the European Convention on Human Rights was incorporated into domestic law by the Human Rights Act 1998. This led Lord Steyn in *Reynolds v Times Newspapers Ltd* to comment that, "article 10 of the Convention and the English law on the point are in material respects the same".[6]

6.6 The focus in this chapter will nevertheless be on Article 10 of the European Convention on Human Rights rather than the common law to reflect the fact that the lawfulness of provisions that criminalise expression have, since the Human Rights Act 1998 came into force, most commonly been assessed against Article 10.[7]

6.7 There are at least two reasons why it is necessary to consider the impact that unauthorised disclosure offences have upon freedom of expression. First, we want to ensure that any proposals for reform that we make are compatible with the European Convention on Human Rights. Secondly, and more specifically, we are keen to ascertain whether ensuring compatibility with the European Convention on Human Rights requires the inclusion of a public interest defence into any provision that criminalises the unauthorised disclosure of information. The extent to which the defence is and should be available to disclosure offences is considered in the next chapter.

ARTICLE 10 OF THE EUROPEAN CONVENTION ON HUMAN RIGHTS

6.8 Article 10 of the European Convention on Human Rights provides that:

> Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This Article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises.
>
> The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary.

[5] *Reynolds v Times Newspapers Ltd and Others* [2001] 2 AC 127, 207-208, by Lord Steyn. See also Human Rights Act 1998, s 12.

[6] *Reynolds v Times Newspapers Ltd and Others* [2001] 2 AC 127, 207, by Lord Steyn.

6.9 This section will first examine the general principles that apply to Article 10, which will demonstrate that freedom of expression is not an absolute right. Then we will examine how the right to freedom of expression has been interpreted by both domestic courts and the European Court of Human Rights. We explore the approach that is taken when the courts are considering whether a provision that infringes freedom of expression violates the European Convention on Human Rights.

Freedom of expression – general principles

6.10 The European Court of Human Rights has emphasised in many cases that the right to freedom of expression is an "essential foundation of a democratic society" and a "basic condition for its progress and for the development of every man".[8]

6.11 Richard Clayton and Hugh Tomlinson describe the fundamental principles that apply in the following terms.

> Freedom of expression constitutes one of the essential foundations of a democratic society and one of the basic conditions for its progress and for each individual's self-fulfilment. Subject to Article 10(2), it is applicable not only to "information" or "ideas" that are favourably received or regarded as inoffensive or as a matter of indifference, but also to those that offend, shock or disturb. Such are the demands of pluralism, tolerance and broadmindedness without which there is no "democratic society". As set forth in Article 10, this freedom is subject to exceptions, which must, however, be construed strictly, and the need for any restrictions must be established convincingly.
>
> The adjective "necessary", within the meaning of Article 10(2), implies the existence of a "pressing social need" for any qualification to the right. The European Court of Human Rights has acknowledged that the Contracting States have a certain margin of appreciation in assessing whether such a need exists, but it goes hand in hand with European supervision, embracing both legislation and the decisions applying it, even those given by an independent court.[9] The European Court of Human Rights is therefore empowered to give the final ruling on whether a "restriction" is reconcilable with freedom of expression as protected by Article 10.
>
> The task of the European Court of Human Rights, in exercising its supervisory jurisdiction, is not to take the place of the competent national authorities but rather to review under Article 10 the decisions

7 For general consideration of freedom of expression under both the common law and the Convention see B Emmerson, A Ashworth and A Macdonald (eds), *Human Rights and Criminal Justice* (3rd edn 2012) ch 18 paras 20-62.

8 *Handyside v United Kingdom* (1979-80) 1 EHRR 737 at [49].

9 Emmerson, Ashworth and Macdonald describe the margin of appreciation as, "a doctrine of restrained review at the international level, which reflects the primary role that the national authorities, including the courts, are intended to perform in human rights protection" See further B Emmerson, A Ashworth and A Macdonald (eds), *Human Rights and Criminal Justice* (3rd edn 2012) paras 2-115-2-138.

> they delivered pursuant to their power of appreciation. This does not mean that the supervision is limited to ascertaining whether the respondent State exercised its discretion reasonably, carefully and in good faith; what the court has to do is look at the interference complained of in the light of the case as a whole and determine whether it was "proportionate to the legitimate aim pursued" and whether the reasons adduced by the national authorities to justify it are "relevant and sufficient". In doing so, the court has to satisfy itself that the national authorities applied standards which were in conformity with the principles embodied in Article 10 and, moreover, that they relied on an acceptable assessment of the relevant facts.[10]

6.12 The term "expression" is interpreted by the European Court of Human Rights broadly. Apart from a small number of exceptions, no form of expression is excluded from the scope of Article 10 on the basis of its content.[11]

6.13 In relation to whether Article 10 extends to employees, which is of direct relevance to the topic under consideration in this paper, it is sometimes said that an employee can contract out of his or her right to freedom of expression. This claim, however, has been questioned.[12] According to Clayton and Tomlinson, the better view is that, although employees' rights to freedom of expression can be restricted by contract, this is always subject to scrutiny by the courts.[13] The European Court of Human Rights has recognised, however, that there are some types of employment which, by their nature, involve restrictions on freedom of expression. By way of example, in *Hadjianastassiou v Greece* it was held that there had been no violation of Article 10 when an officer of the Greek Air Force was found guilty of disclosing military secrets. Importantly for present purposes, the European Court of Human Rights stated that:

> It is also necessary to take into account the special conditions attaching to military life and the specific 'duties' and 'responsibilities' incumbent on the members of the armed forces. The applicant, as the officer at the KETA [i.e. the Greek Air Force] in charge of an experimental missile programme, was bound by an obligation of discretion in relation to anything concerning the performance of his duties.[14]

6.14 This is relevant for present purposes because many of the offences considered in this paper can only be committed by Crown servants and others whose occupation necessarily entails a restriction on their freedom of expression.

Justifying restrictions on freedom of expression

6.15 The right to freedom of expression is not absolute. An interference with the right to freedom of expression will comply with the European Convention on Human

[10] Direct quotation from R Clayton and H Tomlinson, *The Law of Human Rights* (2nd ed 2010) ch 15, para 239.

[11] For further discussion see M Amos, *Human Rights Law* (2nd ed 2014) pp 553-555.

[12] R Clayton and H Tomlinson, *The Law of Human Rights* (2nd ed 2010) ch 15 para 246.

[13] R Clayton and H Tomlinson, *The Law of Human Rights* (2nd ed 2010) ch 15 para 246.

Rights provided all of the following criteria are satisfied. These criteria are set out in Article 10(2) of the European Convention on Human Rights:

(1) The interference was prescribed by law.

(2) The interference sought to pursue one of the legitimate aims listed in Article 10(2).

(3) The interference was necessary in a democratic society.

6.16 The following section of this chapter will examine how the European Court of Human Rights has interpreted each of these criteria.

Was the interference prescribed by law?

6.17 An interference will be "prescribed by law" where:

(1) the interference in question has some basis in domestic law;

(2) the law is adequately accessible; and

(3) the law is formulated so that it is sufficiently foreseeable.[15]

6.18 In *Sunday Times v United Kingdom* it was held that the citizen must be able to foresee, if necessary with "appropriate advice", the legal consequence a given action may entail.[16]

6.19 We believe that these criteria are easily satisfied by the provisions we are examining in this paper, given that there is no ambiguity around the fact a criminal offence will be committed if certain categories of information are disclosed without authorisation.

Did the interference pursue a legitimate aim?

6.20 An interference will only be justified if it was in pursuance of one of the legitimate aims listed in Article 10(2) as set out above. Clayton and Tomlinson state that in practice there are few disputes about whether an interference falls within the scope of one or more of the listed aims.[17] They do suggest, however, that the legitimate aim relied upon will be relevant to the breadth of the "margin of appreciation" the European Court of Human Rights afford the state.[18]

6.21 In the context of unauthorised disclosure offences, there are two legitimate aims that are relevant: national security; and the protection of the reputation and rights of others.

[14] *Hadjianastassiou v Greece* (1993) 16 EHRR 219 at [46].

[15] R Clayton and H Tomlinson, *The Law of Human Rights* (2nd ed 2010) ch 15 para 299.

[16] *Sunday Times v United Kingdom* (1979-80) 2 EHRR 245 at [49].

[17] R Clayton and H Tomlinson, *The Law of Human Rights* (2nd ed 2010) ch 15 para 305.

[18] R Clayton and H Tomlinson, *The Law of Human Rights* (2nd ed 2010) ch 15 para 305.

Necessary in a democratic society

6.22 It is important to note that the reference to necessity in Article 10(2) does not mean "indispensable". The task of the European Court of Human Rights is to evaluate whether the interference complained of corresponded to a "pressing social need", whether it was proportionate to the legitimate aim pursued and finally whether the reasons given by the national authority to justify it are relevant and sufficient to justify the interference.

6.23 The following five factors are considered by the European Court of Human Rights when it is evaluating whether an interference with Article 10(1) is justified:

(1) The value of the type of expression;

(2) The medium of expression;

(3) The audience or target of the expression;

(4) The objective of the interference; and

(5) The nature of the interference, in particular the nature of the sanctions imposed.[19]

6.24 It is important to bear in mind that when considering whether an interference is justified, the European Court of Human Rights will accord the national authority a certain "margin of appreciation". The extent of this margin of appreciation will, however, depend upon the nature of the expression involved and the legitimate aim relied upon by the national authority.[20]

6.25 As we have already commented, the two justifications most likely to be relied upon in the present context are national security, and the protection of the reputation or rights of others. Different considerations apply to different aims and the margin of appreciation accorded by the European Court of Human Rights can vary, depending upon the justification being advanced by domestic authorities.

THE OFFICIAL SECRETS ACT 1989 AND FREEDOM OF EXPRESSION

6.26 Having set out the applicable principles, this section will consider the relationship between the Official Secrets Act 1989 and Article 10. This analysis will be crucial in ensuring that our options for reform are compatible with the European Convention on Human Rights.

6.27 The only case, of which we are aware, to consider whether the Official Secrets Act 1989 is compatible with Article 10 of the European Convention on Human Rights is *Shayler*.[21] It important to note that, as it has never been overturned by the Supreme Court, the judgment in *Shayler* remains binding in domestic law.

6.28 The defendant was a former member of the Security Service who disclosed to a newspaper information obtained in the course of his employment. Having done

[19] R Clayton and H Tomlinson, *The Law of Human Rights* (2nd ed 2010) ch 15 para 306.

[20] S Turenne, "The Compatibility of Criminal Liability with Freedom of Expression" (2007) *Criminal Law Review* 866.

so, he was charged with offences contrary to sections 1(1)(a), 4(1) and 4(3) of the Official Secrets Act 1989. A preliminary question arose as to whether compatibility with Article 10 required the defendant to be able to plead that the disclosure was in the public interest.

6.29 In rejecting this argument, Lord Bingham began by observing that:

> The need to preserve the secrecy of information relating to intelligence and military operations in order to counter terrorism, criminal activity, hostile activity and subversion has been recognised by the European Commission and the Court in relation to complaints made under article 10 and other articles under the Convention.[22]

6.30 Lord Bingham also cited a number of domestic authorities pointing to the need for the security and intelligence services to work in secret.[23] In support of this proposition, the following passage of Lord Griffiths from *Attorney General v Guardian Newspaper (No 2)* was cited with approval:

> The Security and Intelligence Services are necessary for our national security. They are, and must remain, secret services if they are to operate efficiently. The only practical way to achieve this objective is a brightline rule that forbids any member or ex-member of the service to publish any material relating to his service experience unless he has had the material cleared by his employers. There is, in my view, no room for an exception to this rule dealing with trivia that should not be regarded as confidential. What may appear to the writer to be trivial may in fact be the one missing piece in the jigsaw sought by some hostile intelligence agency.[24]

6.31 Having set out these general principles, Lord Bingham characterised the issue between the defendant and the Crown as being whether the prohibition on disclosure was necessary, fulfilled a pressing social need, and was proportionate.[25]

6.32 In considering these issues, Lord Bingham placed particular emphasis on the fact that the prohibition on disclosure imposed by the Official Secrets Act 1989 is not absolute.[26] Rather, he stated that the Official Secrets Act 1989 imposes a prohibition on disclosure *without lawful authority*. Lord Bingham then proceeded to set out the office holders to whom a former member of the security and intelligence agencies could make a lawful disclosure:

[21] *R v Shayler* [2002] UKHL 11, [2003] 1 AC 247.

[22] *R v Shayler* [2002] UKHL 11, [2003] 1 AC 247 at [26].

[23] *R v Shayler* [2002] UKHL 11, [2003] 1 AC 247 at [25].

[24] *R v Shayler* [2002] UKHL 11, [2003] 1 AC 247 at [25] citing *Attorney General v Guardian Newspaper (No 2)* [1990] 1 AC 109, 269, by Lord Griffiths (HL).

[25] *R v Shayler* [2002] UKHL 11, [2003] 1 AC 247 at [30].

[26] *R v Shayler* [2002] UKHL 11, [2003] 1 AC 247 at [27].

(1) The former member may make disclosure to the Staff Counsellor, whose appointment was announced in the House of Commons in November 1987. Lord Bingham characterised the Staff Counsellor as, "a high ranking former civil servant who is available to be consulted by any member of the security and intelligence services who has anxieties relating to the work of his or her service which it has not been possible to allay through the ordinary processes of management-staff relations". We examine in greater detail the role played by the Staff Counsellor in the next chapter.

(2) If the former member has concerns about the lawfulness of what the service has done or is doing, he or she may disclose his or her concerns to (among others) the Attorney General, the Director of Public Prosecutions or the Commissioner of the Metropolitan Police Service. Lord Bingham stated that these officer holders are under a clear duty, in the public interest, to uphold the law, investigate alleged infractions and prosecute where offences appear to have been committed, irrespective of any party affiliation or service loyalty.

(3) If a former member has concerns about misbehaviour, irregularity, maladministration, waste of resources or incompetence in the service, Lord Bingham stated that he or she may disclose these to the Home Secretary, the Foreign Secretary, the Secretary of State for Northern Ireland or Scotland, the Prime Minister, the Secretary to the Cabinet or the Joint Intelligence Committee. In addition, Lord Bingham observed that a disclosure could be made to the secretariat to the Intelligence and Security Committee of Parliament. Finally, by virtue of article 3 of, and Schedule 2 to, the Official Secrets Act 1989 (Prescription) Order, a disclosure may be made to the staff of the Comptroller and Auditor General, the National Audit Office and the Parliamentary Commissioner for Administration.[27]

6.33 Having listed the officer holders to whom disclosure could lawfully be made, Lord Bingham stated:

> One would hope that, if disclosure were made to one or other of the persons listed above, effective action would be taken to ensure that abuses were remedied and offenders punished. But the possibility must exist that such action would not be taken when it should be taken or that, despite the taking of effective action to remedy past abuses and punish past delinquencies, there would remain facts which should in the public interest be revealed to a wider audience. This is where, under the OSA 1989 the second condition comes into play: the former member may seek official authorisation to make disclosure to a wider audience.[28]

6.34 Although Lord Bingham expected that official authorisation would only be withheld when an adequate justification existed, he did recognise the possibility

[27] *R v Shayler* [2002] UKHL 11, [2003] 1 AC 247 at [27].

[28] *R v Shayler* [2002] UKHL 11, [2003] 1 AC 247 at [29].

that authorisation could be withheld despite the fact no such justification existed.[29]

6.35 If authorisation was refused, Lord Bingham stated that the individual in question could seek judicial review of this decision. Given that the decision to refuse authorisation impacts upon a right enshrined in the European Convention on Human Rights, Lord Bingham stated that any such refusal must be subject to rigorous scrutiny. For this reason, Lord Bingham rejected the argument that judicial review offered insufficient protection for individuals in the appellant's position.[30]

6.36 Lord Bingham made the following observations about the approach a court would take if judicial review were sought:

> The court's willingness to intervene will very much depend on the nature of the material which it is sought to disclose. If the issue concerns the disclosure of documents bearing a high security classification and there is apparently credible unchallenged evidence that disclosure is liable to lead to the identification of agents or the compromise of informers, the court may very well be unwilling to intervene. If, at the other end of the spectrum, it appears that while disclosure of the material may cause embarrassment or arouse criticism, it will not damage any security or intelligence interest, the court's reaction is likely to be very different. Usually, a proposed disclosure will fall between these two extremes and the court must exercise its judgment, informed by article 10 considerations.[31]

6.37 Lord Bingham also rejected the argument that judicial review was an illusory option, because the applicant would be unable to instruct a lawyer of his choosing without committing further offences. In rejecting this argument, Lord Bingham stated:

> I cannot envisage circumstances in which it would be proper for the service to refuse its authorisation for any disclosure at all to a qualified lawyer from whom the former member wished to seek advice.[32]

6.38 He also cited the requirement of the Attorney General to grant his or her consent before a prosecution can be brought as an additional safeguard. In rejecting the appellant's argument that the role of the Attorney General was not an effective safeguard, Lord Bingham stated:

> The Attorney General will not give his consent to prosecution unless he judges prosecution to be in the public interest. He is unlikely to consent if the disclosure alleged is trivial or the information disclosed stale and notorious or the facts are such as would not be thought by

[29] *R v Shayler* [2002] UKHL 11, [2003] 1 AC 247 at [31].

[30] *R v Shayler* [2002] UKHL 11, [2003] 1 AC 247 at [32]-[34].

[31] *R v Shayler* [2002] UKHL 11, [2003] 1 AC 247 at [33].

[32] *R v Shayler* [2002] UKHL 11, [2003] 1 AC 247 at [34].

> reasonable jurors or judges to merit the imposition of criminal sanctions. The consent of the Attorney General is required as a safeguard against ill-judged or ill-founded or improperly motivated or unnecessary prosecutions.[33]

6.39 Lord Bingham concluded by stating:

> It is plain that a sweeping, blanket ban, permitting of no exceptions, would be inconsistent with the general right guaranteed by article 10(1) and would not survive the rigorous and particular scrutiny required to give effect to article 10(2). The crux of this case is whether the safeguards built into the OSA 1989 are sufficient to ensure that unlawfulness and irregularity can be reported to those with the power and duty to take effective action, that the power to withhold authorisation to publish is not abused and that proper disclosures are not stifled. In my opinion the procedures discussed above, properly applied, provide sufficient and effective safeguards. It is, however, necessary that a member or former member of a relevant service should avail himself of the procedures available to him under the Act. A former member of a relevant service, prosecuted for making an unauthorised disclosure, cannot defend himself by contending that if he had made disclosure under section 7(3)(a) no notice or action would have been taken or that if he had sought authorisation under section 7(3)(b) it would have been refused. If a person who has given a binding undertaking of confidentiality seeks to be relieved, even in part, from that undertaking he must seek authorisation and, if so advised, challenge any refusal of authorisation.[34]

6.40 In their judgments, Lord Hobhouse, Lord Hutton and Lord Scott agreed with the judgment of Lord Bingham.[35]

6.41 In his judgment, Lord Hope expressed some unease with certain aspects of the Official Secrets Act 1989.[36] He agreed that the Official Secrets Act 1989 did not impose a blanket restriction on disclosure and observed that the class of individuals from whom official authorisation could be obtained in section 7(3) was in fact very wide.[37]

6.42 Lord Hope then proceeded to make the following comments:

> As I see it, the scheme of the Act is vulnerable to criticism on the ground that it lacks the necessary degree of sensitivity. There must, as I have said, be some doubt as to whether a whistle-blower who believes that he has good grounds for asserting that abuses are being perpetrated by the security or intelligence services will be able

[33] *R v Shayler* [2002] UKHL 11, [2003] 1 AC 247 at [35].

[34] *R v Shayler* [2002] UKHL 11, [2003] 1 AC 247 at [36].

[35] *R v Shayler* [2002] UKHL 11, [2003] 1 AC 247 at [119], by Lord Hobhouse, at [87], by Lord Hutton, at [120] by Lord Scott.

[36] *R v Shayler* [2002] UKHL 11, [2003] 1 AC 247 at [40]-[41].

[37] *R v Shayler* [2002] UKHL 11, [2003] 1 AC 247 at [63].

> to persuade those to whom he can make disclosures to take his allegations seriously, to persevere with them and to effect the changes which, if there is substance in them, are necessary.[38]

6.43 Lord Hope was also critical of the fact the legislation does not specify what factors must be taken into consideration when an assessment is being made of whether to grant official authorisation to disclose information.[39] We are confident that the options for reform we propose in the next chapter would remove the doubts expressed by Lord Hope.

6.44 The fact the appellant had not made any effort to test the efficacy of the mechanisms available to him to obtain official authorisation meant, in the view of Lord Hope, that these criticisms of the legislation did not carry the weight they otherwise would have done.[40]

6.45 Despite his misgivings about the legislative regime, Lord Hope concluded that the possibility of judicial review of a decision not to authorise a disclosure ensured that it complied with the requirements of Article 10(2).[41]

6.46 Lord Hope held that the regime established by the Official Secrets Act 1989 came within the:

> wide margin of discretion which is to be accorded to the legislature in matters relating to national security especially where the Convention rights of others such as the right to life may be put in jeopardy.[42]

6.47 It was held that a system mandating authorisation before a disclosure could be made was also optimal for the following reason:

> In favour of that choice there are a number of important factors. However well intentioned he or she may be, a member or former member of the security or intelligence services may not be equipped with sufficient information to understand the potential impact of any disclosure. It may cause far more damage than the person making the disclosure was ever in a position to anticipate. The criminal process risks compounding the potential for damage to the operations of these services, if the prosecution have to prove beyond reasonable doubt the damaging nature of the disclosures.[43]

6.48 Therefore, not only was the system of pre-authorisation Convention compliant, but the fact there was no need for the prosecution to prove that the disclosures made by the appellant were damaging was also held to comply with the Convention.

[38] *R v Shayler* [2002] UKHL 11, [2003] 1 AC 247 at [70].

[39] *R v Shayler* [2002] UKHL 11, [2003] 1 AC 247 at [71].

[40] *R v Shayler* [2002] UKHL 11, [2003] 1 AC 247 at [70].

[41] *R v Shayler* [2002] UKHL 11, [2003] 1 AC 247 at [85].

[42] *R v Shayler* [2002] UKHL 11, [2003] 1 AC 247 at [80].

[43] *R v Shayler* [2002] UKHL 11, [2003] 1 AC 247 at [84], by Lord Hope.

6.49 The speeches of the various Law Lords in *Shayler* have been the subject of criticism. Helen Fenwick and Gavin Phillipson are critical of the judgment of Lord Bingham, as they believe he did not consider the proportionality test in sufficient detail.[44] They suggest that Lord Bingham simply assumed that once it was demonstrated that the prohibition on disclosure was not a blanket one, proportionality was automatically satisfied. They disagree with this assumption.

6.50 Fenwick and Phillipson are also critical of the fact there was no detailed examination of whether the routes available to obtain authorisation to disclose information were likely to prove effective. They argue that Lord Bingham's view on this matter seemed naïve.[45] Birkinshaw and Varney have similarly expressed the view that Lord Bingham provided a very optimistic view of the procedures and their efficacy.[46]

6.51 Fenwick and Phillipson are also critical of the fact that Lord Hutton in his judgment placed so much emphasis on the fact the appellant made no effort to avail himself of the routes available to him on the basis that this inverted the proportionality analysis. They argue that the burden should have been on the state to demonstrate that these routes would have been effective, not on the appellant to demonstrate that they were not effective.[47]

6.52 Although Fenwick and Phillipson are less critical of Lord Hope's judgment, they nevertheless conclude:

> The basic problem with the reliance placed by all the judges who heard this case upon the internal complaint route and judicial review is that the means they viewed as available to members or former members of the security services to expose inequity are so unlikely to be used it seems, to say the least, highly improbable that such a member would risk the employment detriment that might be likely to arise, especially if he or she then proceeded to seek judicial review of the decision.[48]

6.53 This is speculation, however, and does not accord with the views of the stakeholders we met with during our pre-consultation. Although we do not agree with all of their conclusions, we do agree with Fenwick and Phillipson that it is imperative to ensure that there is a sufficiently robust route available to members of security and intelligence agencies through which they can raise concerns that relate to their work. For now it is sufficient to point out that *Shayler* is authority for the proposition that compliance with Article 10 does not require a public interest defence for those offences contained in the Official Secrets Act 1989. It also demonstrates the importance of having alternative means of raising a concern.

[44] H Fenwick and G Phillipson, *Media Freedom under the Human Rights Act* (2006) p 941.

[45] H Fenwick and G Phillipson, *Media Freedom under the Human Rights Act* (2006) p 941.

[46] P Birkinshaw and M Varney, *Government and Information: The Law Relating to Access, Disclosure and their Regulation* (4th ed 2011) p 208.

[47] H Fenwick and G Phillipson, *Media Freedom under the Human Rights Act* (2006) p 941.

[48] H Fenwick and G Phillipson, *Media Freedom under the Human Rights Act* (2006) p 943.

6.54 It is important at this stage to point out that not every commentator is critical of the approach taken in *Shayler*. For example, Dickson has stated:

> The lack of any public interest defence in the Official Secrets Act 1989, however, is still a cause for widespread criticism. But it is likely that if a challenge were taken to Strasbourg on this point it would fail. This is an area where the United Kingdom's top court seems to have faithfully applied the tests set out by the European Court of Human Rights for deciding whether an interference with Article 10(1) rights is justified.[49]

Other disclosure offences and freedom of expression

6.55 As we discussed in Chapter 4, the offences contained in the Official Secrets Act 1989 are not the only offences that criminalise the unauthorised disclosure of information. We are not aware of any cases, however, in which a court has had to consider whether these other offences are compatible with Article 10 of the European Convention on Human Rights.

6.56 The extent to which these offences are compatible with Article 10 requires consideration of different legitimate aims. For example, the offences in section 55 of the Data Protection Act 1998 could be characterised as protecting the rights of others, in particular the right to privacy enshrined in Article 8 of the European Convention on Human Rights. The offence contained in section 79 of the Anti-Terrorism, Crime and Security Act 2001, which relates to nuclear sites and nuclear material, would engage a different legitimate interest, namely national security.

6.57 Despite the fact that these provisions pursue different legitimate aims, when considering how they relate to Article 10 of the European Convention on Human Rights, a court would still apply the process we have set out above. We believe therefore that our conclusions in this section would apply to those offences that criminalise the unauthorised disclosure of information that relates to national security.

MORE RECENT DEVELOPMENTS IN THE CASE LAW OF THE EUROPEAN COURT OF HUMAN RIGHTS

6.58 The judgment of the House of Lords in *Shayler* remains binding and is direct authority for the proposition that compliance with Article 10 does not require the availability of a public interest defence for those offences contained in the Official Secrets Act 1989.

6.59 There are a number of more recent judgments of the European Court of Human Rights in which the court has sought to clarify the principles that apply when considering the relationship between Article 10 and disclosures made by those who work in the public sector. Although *Shayler* remains authoritative as a matter of domestic law, in this section we consider whether these more recent developments would necessitate a different approach.

[49] B Dickson, *Human Rights and the United Kingdom Supreme Court* (2013) p 290.

6.60 In *Guja v Moldova* the applicant disclosed to a newspaper internal letters that demonstrated political interference with decisions concerning whether to prosecute individuals for criminal offences.[50] When it was discovered that he was the source of the disclosures, the applicant was dismissed from his job in the Prosecutor General's Office. This is not, therefore, a case in which the discloser of the information was prosecuted for a criminal offence, however, the European Court of Human Rights has relied upon the principles articulated in *Guja v Moldova* in subsequent criminal cases.[51]

6.61 The question for the Grand Chamber of the European Court of Human Rights was whether the interference with the applicant's right to freedom of expression was proportionate to the aim pursued. The European Court of Human Rights enunciated the following five principles it stated ought to apply when determining the proportionality of an interference with a civil servant's freedom of expression. The court did not specify the weight that ought to be attached to each principle.

(1) The public interest in the disclosed information - The Grand Chamber stated that the interest which the public may have in particular information can sometimes be so strong so as to override even a legally imposed duty of confidence. The court did not, however, provide further elucidation of what the term "public interest" means in this context, how it ought to be assessed or by whom.[52]

(2) The authenticity of the information disclosed - It was observed that the state has the right to challenge defamatory or untrue information. A burden is therefore placed on the discloser of the information to ensure it is accurate.[53]

(3) The damage, if any, suffered by the public authority as a result of the disclosure in question - The Grand Chamber held that it must assess whether such damage outweighed the interest of the public in having the information revealed. It was also held that the subject-matter of the disclosure and the nature of the administrative authority concerned may be relevant.[54]

(4) The motive behind the action of the reporting employee - The Grand Chamber observed that an act motivated by a personal grievance or a personal antagonism; or with the expectation of personal advantage, including pecuniary advantage; would not justify a particularly strong degree of protection.[55]

[50] *Guja v Moldova* (2011) 53 EHRR 16.

[51] See for example *Marchenko v Ukraine* (2010) 51 EHRR 36 where the applicant successfully argued that his conviction for defamation under the Ukrainian criminal code was contrary to Article 10 as his disclosure to the public was a last resort.

[52] *Guja v Moldova* (2011) 53 EHRR 16 at [85]-[88].

[53] *Guja v Moldova* (2011) 53 EHRR 16 at [89].

[54] Given that damage is based on weighing the total consequences of an action, this third principle would appear to be intimately linked to the first principle.

[55] *Guja v Moldova* (2011) 53 EHRR 16 [92]–[94].

(5) The Grand Chamber held that close attention must be paid to the penalty imposed and its consequences.[56]

6.62 Importantly, the Grand Chamber also held:

> In the light of the duty of discretion referred to above, disclosure should be made in the first place to the person's superior or other competent authority or body. It is only where this is clearly impracticable that the information could, *as a last resort,* be disclosed to the public. In assessing whether the restriction on freedom of expression was proportionate therefore, the Court must take into account whether there was available to the applicant any other effective means of remedying the wrongdoing which he intended to uncover.[57]

6.63 It is unclear whether the court intended for the existence of other competent bodies to be a threshold question that must be answered in the affirmative before the other principles are considered or whether this is merely a further principle that must be considered alongside the others. In other words, if the disclosure was patently not a last resort, must the court still consider the above five listed principles?

6.64 The Grand Chamber did make clear in *Guja v Moldova*, however, that public disclosure should be a last resort. In coming to the conclusion that the interference with the applicant's rights under Article 10(1) was not proportionate in *Guja v Moldova*, the Grand Chamber placed particular emphasis on the fact there was no authority other than his superiors to whom the applicant could have reported his concerns and no prescribed procedure for reporting such matters. What is tolerably clear from *Guja v Moldova* is that the existence of an alternative to disclosing the information is crucial.

6.65 Before leaving *Guja v Moldova*, it is necessary to point out that the legitimate aim being pursued by the Government was characterised as preventing the disclosure of information received in confidence.[58] This was therefore not a case concerning national security. Given that the European Court of Human Rights tends to accord a wider margin of appreciation in cases concerning national security,[59] *Guja v Moldova* is merely indicative of the approach the court would take in a case in which the national authorities invoked national security as the legitimate aim to justify the interference with Article 10(1).

6.66 The European Court of Human Rights has reaffirmed more recently the need to consider the availability of effective means to remedy the wrongdoing the applicant sought to bring to the attention of the public. For example, the court in *Heinisch v Germany* has cited with approval the passage from the Grand Chamber in *Guja v Moldova* above, making the following observation:

[56] *Guja v Moldova* (2011) 53 EHRR 16 at [95]–[96].

[57] *Guja v Moldova* (2011) 53 EHRR 16 at [73] (emphasis added).

[58] *Guja v Moldova* (2011) 53 EHRR 16 at [59].

[59] By way of example, see *Hadjianastassiou v Greece* (1993) 16 EHRR 219.

> Consequently, in the light of this duty of loyalty and discretion, disclosure should be made in the first place to the person's superior or other competent authority or body. It is only where this is *clearly impracticable* that the information can*, as a last resort*, be disclosed to the public. In assessing whether the restriction on freedom of expression was proportionate, the Court must therefore take into account whether the applicant had any other effective means of remedying the wrongdoing which he or she intended to uncover.[60]

6.67 The most recent case to consider this issue is *Bucur v Romania*.[61] In this case the applicant worked in the government department responsible for monitoring and recording telephone communications. The department was located within a unit operated by the Romanian intelligence service in the immediate aftermath of the collapse of the Communist regime. One of the applicant's duties was to ensure compliance with the conditions that had to be satisfied in order for communications to be intercepted lawfully, such as keeping up to date the register of persons whose communications were to be intercepted. In the course of his duties, the applicant noted several irregularities. For example, some of the information in the register was missing or incomplete. The applicant also discovered that the communications of a large number of journalists, politicians and prominent business people were being intercepted.

6.68 The applicant brought these irregularities to more senior colleagues and the head of his department. He was reprimanded, however, and advised to retract the allegations of impropriety. The applicant then brought the matter to the attention of his Member of Parliament, who was also a member of the parliamentary commission with responsibility for overseeing the work of the Romanian intelligence service. The applicant was advised that the links between the director of the Romanian intelligence service and the head of the parliamentary commission meant that his allegations of impropriety were likely to be ignored. For this reason, the applicant was advised to hold a press conference to bring the alleged improprieties to the attention of the public. The applicant did so and was charged with a number of criminal offences. After a protracted trial, he was convicted in a military court and given a suspended sentence of two years' imprisonment. The applicant's conviction was upheld by the Romanian Supreme Court.

6.69 Before the European Court of Human Rights, the applicant argued that his conviction violated his right to freedom of expression, enshrined in Article 10(1) of the European Convention on Human Rights. The Government conceded that the applicant's conviction violated Article 10(1), but argued that it fell within the terms of Article 10(2).

6.70 The European Court of Human Rights accepted that the violation pursued a legitimate aim, namely the deterrence and punishment of offences relating to

[60] *Heinisch v Germany* (2014) 58 EHRR 31 at [65] (emphasis added). See also, *Marchenko v Ukraine* (2010) 51 EHRR 36.

[61] *Bucur and Toma v Romania* App No 40238/02.

national security. The question of whether the interference was necessary in a democratic society caused the court greater difficulty.[62]

6.71 In assessing the proportionality of the interference, the European Court of Human Rights placed a great deal of reliance upon the test enunciated by the Grand Chamber in *Guja v Moldova.* As we have discussed already, the approach articulated by the Grand Chamber requires the court to assess whether the applicant had less damaging ways to make the disclosure available to him or her. Given the fact the applicant was rebuffed by his superiors when he attempted to bring the impropriety to their attention, the European Court of Human Rights concluded:

> The Court further notes that the people responsible for analysing the data collected and for justifying the interception of telephone communications were the applicant's superiors, and the irregularities therefore directly concerned them. In these circumstances, the Court doubts the effectiveness of any report that the applicant could have made to his superiors… Therefore, the Court is not convinced that any internal complaints lodged by the applicant would have resulted in an investigation into and the cessation of the irregularities.[63]

6.72 Given the fact that a member of the parliamentary oversight commission told the applicant that any referral of the irregularities to the commission would be ineffective, the court concluded that it was not convinced that a formal referral to the committee would have constituted an effective means for reporting irregularities.[64] Therefore, there was no viable option available to the applicant other than a public disclosure in violation of the relevant statutory prohibition.[65]

6.73 When considering the second principle enunciated in *Guja v Moldova*, namely the public interest in the information disclosed by the applicant, the court concluded that there was an undeniable public interest in the public being informed of impropriety in the interception of communications.[66] The public interest in the disclosure of the information was compounded by the fact that Romanian society had until relatively recently been subject to intensive surveillance by the secret services of the communist regime.[67]

6.74 In relation to the other principles enunciated in *Guja v Moldova*, the court concluded that the applicant had reasonable grounds for believing the information he disclosed was true and there was no evidence that he was motivated by personal gain, a grudge or any other hidden agenda.[68] It also concluded that the public interest in disclosing a report of unlawful conduct on the part of the intelligence services outweighed the desirability of maintaining public confidence

[62] *Bucur and Toma v Romania* App No 40238/02 at [92].

[63] *Bucur and Toma v Romania* App No 40238/02 at [97].

[64] *Bucur and Toma v Romania* App No 40238/02at [98].

[65] *Bucur and Toma v Romania* App No 40238/02at [100].

[66] *Bucur and Toma v Romania* App No 40238/02 at [101].

[67] *Bucur and Toma v Romania* App No 40238/02 at [101].

[68] *Bucur and Toma v Romania* App No 40238/02 at [105]-[113] and [116]-[117].

in the institution.[69] Finally, the European Court of Human Rights noted that the sentence imposed by the national court had had a very detrimental impact upon the applicant.[70]

6.75 These factors led the court to find that the infringement of the applicant's right to freedom of expression was not necessary in a democratic society.[71] Article 10 was therefore violated. The Court ordered the state to pay the applicant 20,000 Euro in damages.

6.76 As we have discussed, the House of Lords in *Shayler* rejected the argument that the offences contained in the Official Secrets Act 1989 violated Article 10. Our analysis of the more recent case law of the European Court of Human Rights leads us to conclude that, if the Official Secrets Act 1989 were to be challenged today, the European Court of Human Rights would be likely to conclude that the approach of the House of Lords in *Shayler* remains valid. More specifically, we do not believe that the absence of a statutory public interest defence within the Official Secrets Act 1989 would lead the European Court of Human Rights to find a violation of Article 10.

Provisional conclusion 22

6.77 **Compliance with Article 10 of the European Convention on Human Rights does not mandate a statutory public interest defence. Do consultees agree?**

6.78 We do believe that it is clear that the European Court of Human Rights has expressed the need to ensure that a robust process exists that enables concerns about illegality and impropriety to be raised and that acts as a viable alternative to making a public disclosure. Whilst the House of Lords in *Shayler* expressed confidence in the mechanisms currently in place, as the next chapter will consider, we believe there are ways they could be improved.

[69] *Bucur and Toma v Romania* App No 40238/02 at [114]-[115].

[70] *Bucur and Toma v Romania* App No 40238/02 at [119].

[71] *Bucur and Toma v Romania* App No 40238/02 at [120].

CHAPTER 7
PUBLIC INTEREST DEFENCE

INTRODUCTION

7.1 The extent to which offences that criminalise the unauthorised disclosure of information ought to include a public interest defence has pervaded discussion of this area of the law for decades.[1] This issue is complex and involves detailed consideration of a number of broad issues of policy and principle. It is for these reasons that we have decided to devote a separate chapter to the question of whether any offences that we might recommend to replace those contained in the current legislative regime ought to include a public interest defence.

7.2 This chapter first examines the existing law and the extent to which public interest is currently relevant to the offences considered in this consultation paper. It then discusses three models for incorporating considerations of the public interest into the statutory regime that criminalises unauthorised disclosures: the statutory public interest defence model, the statutory commissioner model, and the Canadian model. Our provisional conclusion is that the commissioner model is the optimal model.

7.3 At the outset it is necessary to point out that there are two versions of public interest defence that may be envisaged. The first type would require an assessment of whether the disclosure was in fact in the public interest. The second type would require an assessment of whether the defendant had a genuine belief that the disclosure would be in the public interest. Strictly speaking, only the former constitutes a true public interest defence, given that the latter is not in fact concerned with the public interest, but rather with what the defendant believed to be in the public interest. Both of these formulations will be considered when evaluating the merits of introducing a public interest defence.

THE CURRENT LAW

7.4 This section examines the extent to which the offences that currently criminalise unauthorised disclosures of protected information provide for public interest defences.

7.5 At this stage it is important to explain the distinction between a "defence" and an "exemption", as the current law contains examples of each. Where a "defence" applies, this means that an individual has committed all the elements of the offence in question, but if certain factors are present they may be absolved of criminal liability. An "exemption" is different, as it means that an individual commits no offence if their disclosure falls within a specified category. For example, as we discussed earlier, in the Investigatory Powers Act a disclosure made to a legal adviser for the purpose of seeking legal advice is an "exempt disclosure". This means that making such a disclosure does not constitute a criminal offence.

[1] By way of example see, S Palmer, "Tightening secrecy law: the Official Secrets Act 1989" [1990] *Public Law* 243; J Griffith, "The Official Secrets Act 1989" [1989] *Journal of Law and Society* 273; A Bailin, "The last Cold War statute" [2008] *Criminal Law Review* 625.

The Official Secrets Act 1989

7.6 None of the disclosure offences contained in the Official Secrets Act 1989 include a public interest defence. The case for including such a defence was considered in the White Paper that preceded the 1989 Act:

> The Government recognises that some people who make unauthorised disclosures do so for what they themselves see as altruistic reasons and without desire for personal gain. But that is equally true of some people who commit other criminal offences. The general principle which the law follows is that the criminality of what people do ought not to depend on their ultimate motives - though these may be a factor in sentencing - but on the nature and degree of the harm which their acts cause.[2]

7.7 The White Paper concluded that there was no reason to depart from this principle in the context of the unauthorised disclosure of information intended to be criminalised by the new legislation.[3] It was suggested that to do so would be contrary to the aim of clarifying which unauthorised disclosures were criminalised. Since the reforms were intended to narrow criminalisation to situations where the disclosure would demonstrably be against the public interest, it was also suggested that including a public interest defence would be contrary to the aims of the legislation.[4]

7.8 The White Paper stated that any argument as to the impact of the disclosure upon the public interest should take place within the assessment of whether the disclosure was damaging.

Data Protection

7.9 The offence in section 55 of the Data Protection Act 1998 is one of the very few criminal offences that includes a public interest defence. It is defined in the following terms:

> (2) Subsection (1) [which sets out the offence] does not apply to a person who shows—
>
> …
>
> (d) that in the particular circumstances the obtaining, disclosing or procuring was justified as being in the public interest.

7.10 The Data Protection Act 1998 was enacted to give effect to the European Union Data Protection Directive.[5] The origin of the defence, however, is difficult to discern. The Directive did not require an offence of unauthorised disclosure to be introduced. Therefore it cannot be said that the inclusion of a public interest defence was mandated by European Union law. Further, the defence is not

[2] Reform of Section 2 of the Official Secrets Act 1911 (1988) Cm 408, para 60.

[3] Reform of Section 2 of the Official Secrets Act 1911 (1988) Cm 408, para 60.

[4] Reform of Section 2 of the Official Secrets Act 1911 (1988) Cm 408, para 61.

[5] Data Protection Directive 95/46/EC.

directly commented upon in the proposals and report that preceded the 1998 Act.[6] Therefore the rationale for the inclusion of a public interest defence is not easy to determine based on the legislation's history.

7.11 Our research has revealed only a small number of judgments in which the public interest defence in section 55(2)(d) has even been tangentially mentioned. There is brief commentary on the defence in *Imerman v Tchenguiz and others.*[7] This case concerned the obtaining of personal information in the context of divorce proceedings. In his judgment, Lord Neuberger remarked that merely protecting one person's rights does not satisfy the threshold of acting in the public interest under the defence:

> Nor does section 55(2)(d) look a particularly promising avenue for the defendants: the fact that accessing the documents can be said to have been to protect Mrs Imerman's rights can scarcely be said to render it "in the public interest" , even if it was done with a view to exposing, or preventing, Mr Imerman's anticipated wrongful concealment of assets.[8]

7.12 Although *Imerman v Tchenguiz and others* is useful for indicating when the public interest defence has not been made out, it does not provide much insight into the circumstances in which the defence is more likely to be successful. Our preliminary consultation with stakeholders confirmed that the defence is pleaded very rarely.

7.13 Section 78 of the Criminal Justice and Immigration Act 2008 inserts a new defence into the offence in section 55 of the 1998 Act. The defence applies if the defendant is acting with a view to publishing "journalistic, literary or artistic material" and they have a reasonable belief that the disclosure, obtaining or procurement of the personal data was in the public interest. This amendment would extend the public interest defence as it applies to those engaged in journalistic activity. The requirement for the defendant to have a reasonable belief means that he or she would be able to plead the defence even if, objectively speaking, the disclosure, obtaining or procuring was not in the public interest. Section 78, however, is not yet in force.

Miscellaneous unauthorised disclosure offences

7.14 Other disclosure offences contain narrowly confined public interest exemptions, rather than defences. Examples include section 20 of the Commissioners for Revenue and Customs Act 2005 and section 3 of the Agricultural Statistics Act 1979. The offences to which both of these exemptions relate concern the disclosure of personal information held by the state.

7.15 Section 20 of the 2005 Act provides that a disclosure is in the public interest when the Commissioners for Her Majesty's Revenue and Customs are satisfied it

[6] Home Office, Consultation Paper on the EC Data Protection Directive (95/46/EC) (March 1996); Data Protection: the Government Proposals (1997) Cm 3725.

[7] *Imerman v Tchenguiz* [2010] EWCA Civ 908; [2011] Fam 116.

[8] *Imerman v Tchenguiz* [2010] EWCA Civ 908; [2011] Fam 116 at [103].

is in the public interest. Public interest is defined with reference to a set of narrowly defined circumstances. For example:

> (2) This subsection applies to a disclosure made—
>
> > (a) to a person exercising public functions (whether or not within the United Kingdom),
> >
> > (b) for the purposes of the prevention or detection of crime, and
> >
> > (c) in order to comply with an obligation of the United Kingdom, or Her Majesty's Government, under an international or other agreement relating to the movement of persons, goods or services.

7.16 Section 3 of the 1979 Act is structured in a similarly narrow way:

> (1) If the disclosure is confined to situation, extent, number and kind of livestock, character of land, and name and address of owner and occupier, to any person to whom the appropriate Minister considers that the disclosure is required in the public interest.

7.17 In both of these examples, the public interest is defined narrowly and is determined by either a Minister or one of the Revenue and Customs Commissioners. These are unusual provisions and are not representative of how a public interest defence is typically understood.

The Public Interest Disclosure Act 1998

7.18 The defences and exemptions considered in the previous sections, if pleaded successfully, absolve the defendant of criminal liability. It is necessary to consider the provisions contained in the Public Interest Disclosure Act 1998. The Act inserts the following into the Employment Rights Act 1996:

> A worker has the right not to be subjected to any detriment by any act, or any deliberate failure to act, by his employer done on the ground that the worker has made a protected disclosure.[9]

7.19 It is necessary to emphasise, however, that disclosures which constitute a criminal offence are not protected by the 1998 Act.[10] The Public Interest Disclosure Act 1998 amended the Employment Rights Act 1996 to increase protection for those who make public interest disclosures. It applies to employees in both the public and private sectors.[11] Not every disclosure, however, qualifies for protection. For a disclosure to qualify, the individual who makes it must have a reasonable belief that it demonstrates one of the following categories of behaviour has occurred, is occurring or will occur:

(1) a criminal offence;

[9] Employment Rights Act 1996, s 47B

[10] Employment Rights Act 1996, s 43B.

(2) a failure to comply with any legal obligation;

(3) a miscarriage of justice;

(4) the endangerment of an individual's health or safety;

(5) environmental damage; or

(6) deliberate concealment of information tending to show any matter falling within any of the above categories.

7.20 The 1998 Act as amended by section 17 of the Enterprise and Regulatory Reform Act 2013 first requires the discloser reasonably to believe that the disclosure was in the public interest.

7.21 The disclosure must also satisfy the requirements for one of the forms of disclosure permitted by the Act. The Act allows for disclosures to be made if they fall within one of the "steps" provided for in the Act.[12] Savage describes these steps as follows:

> The first step allows for concerns to be raised internally to an employer, line manager or person designated by a policy to receive a concern. The second step allows for disclosures to be made externally to a prescribed person. The third allows for disclosures to be made to anyone else, thus agencies or bodies who are not prescribed, the police, the media and members of the public.[13]

7.22 If a disclosure is made that falls within the terms of the legislation, then a worker cannot suffer detriment for having made it. For example, they cannot be dismissed by their employer. The Public Interest Disclosure Act 1998 does not extend to members of the security and intelligence services and military personnel.[14]

EVALUATING THE MERITS OF A PUBLIC INTEREST DEFENCE

7.23 Given our earlier provisional conclusion that the offences currently contained in the Official Secrets Act 1989 ought to be replaced, we believe it is necessary to evaluate whether a public interest defence ought to be included within any new statutory scheme. The analysis in this section applies equally, however, to the question of whether a public interest defence ought to be introduced into the Official Secrets Act 1989, even in the absence of fundamental reform.

7.24 Our research suggests there are three models that could be used explicitly to incorporate the public interest into a statutory regime that criminalises the unauthorised disclosure of specified categories of information:

[11] Employment Rights Act 1998, s 43(k).

[12] A Savage, *Leaks, Whistleblowing and the Public Interest: The Law on Unauthorised Disclosures* (2016), pp 147 – 156.

[13] A Savage, *Leaks, Whistleblowing and the Public Interest: The Law on Unauthorised Disclosures* (2016), p 141.

[14] Employment Rights Act 1996, s 193.

(1) A statutory public interest defence – as we discussed earlier, broadly speaking, there are two versions of this defence. One is objective and the other is subjective. The objective version would enable an individual charged with disclosing information without lawful authority to argue in their defence that the public interest in disclosing the information in fact outweighed the public interest in maintaining its confidence. If the prosecution failed to make the jury sure that this was not the case, then the defendant would be acquitted. Alternatively, the defendant would be required to demonstrate that they held a genuine belief that the public interest in disclosing the information outweighed the public interest in maintaining its confidence.

(2) The statutory commissioner model – this would enable an individual who might otherwise feel compelled publicly to disclose protected information (for example, due to concerns about illegality or impropriety) to bring this concern to the attention of a statutory commissioner independent of their organisation. This commissioner would be under a statutory duty to investigate the allegation and equally a statutory obligation would be placed upon the relevant parties to assist the investigation.[15] The commissioner would also have an obligation to report to government, subject to the need to ensure information relating to national security is not disclosed to those who are unauthorised to receive such information. This model would safeguard the public interest by ensuring allegations of impropriety or illegality are investigated.

(3) The "Canadian model" – an individual who discloses information without lawful authority would only be able to plead that the disclosure was in the public interest if they have exhausted the other mechanisms that were available to bring the wrongdoing to light. Such mechanisms may include reporting the information to a statutory commissioner, as in the commissioner model. The Canadian model therefore represents a combination of the first two models.

7.25 Before proceeding to examine these it is important to point out that the suitability of each model could be to some extent contingent upon the nature of the offence to which it would apply. This much is evident from the previous reviews that have considered this issue. For example, it could be argued that the need for a statutory public interest defence was far greater when the excessively wide offence in section 2 of the Official Secrets 1911 criminalised the disclosure of all official information.

7.26 In this regard, it is also important to bear in mind our terms of reference, which state that we are to evaluate whether there are any deficiencies in the law and research options for improving the protection of official information. At the heart of this debate is the tension between national security – the need to protect official information and prevent harm to the interests of the state – and government accountability – by promoting transparency and exposing government wrongdoing which is in the public interest. When evaluating the merits of these

[15] The existence of such a mechanism is required by the Tshwane Principles. See African Freedom of Information Centre and others, *The Global Principles on National Security and the Right to Information (Tshwane Principles)* (2013), p 54.

three models in the following sections, it is our aim to balance both these interests.

Model 1: A statutory public interest defence

7.27 This model would introduce a statutory public interest defence. This section evaluates the reasons that could be relied upon to justify the introduction of such a defence, before examining why it could be problematic. The justifications and problems are explored in relation to both the objective and subjective types of defence outlined above. A number of organisations have made the case for the introduction of a statutory public interest defence. For example, the Tshwane Principles, which were drafted following a global consultation led by 22 organisations and academic centres, provide that public personnel should be able to plead a public interest defence to any offence which criminalises the unauthorised disclosure of information. This applies regardless of whether or not an individual had previously made an internal disclosure or a disclosure to an oversight body. This defence would be successful if the public interest in disclosure outweighed the public interest in not disclosing it.[16]

Justifications for the introduction of a statutory public interest defence

7.28 We have identified two reasons that could be invoked to justify introducing a public interest defence:

(1) Enhancing the accountability of government by revealing alleged illegality or impropriety.

(2) Protecting those who make disclosures that they genuinely believe are in the public interest from criminal liability (perhaps irrespective of whether the disclosure was in fact in the public interest).

ENHANCING THE ACCOUNTABILITY OF GOVERNMENT BY REVEALING ALLEGED ILLEGALITY OR IMPROPRIETY

7.29 It has been argued that a public interest defence ought to be introduced because there are some disclosures that serve to enhance the accountability of government by revealing information that ought to be in the public domain, such as illegality or impropriety.[17] For example, as part of her commentary on the White Paper that ultimately led to the Official Secrets Act 1989, Palmer stated:

> A public interest defence raises important ethical issues. Modern governments guard and control vast amounts of material. In the United Kingdom, the executive has a monopoly over official information and has the power to determine what information should become public. But it is not always clear that it is in the public interest for information defined by the government as secret to remain so.

[16] African Freedom of Information Centre and others, *The Global Principles on National Security and the Right to Information (Tshwane Principles)* (2013), pp 55-56.

[17] For example this is central to both Palmer and Bailin's support of the defence. See further S Palmer, "In the Interests of the State: the Government's Proposals for Reforming Section 2 of the Official Secrets Act 1911" [1988] *Public Law* 523; A Bailin, "The Last Cold War Statute" [2008] *Criminal Law Review* 625.

> Disclosures of secret information have in the past served the public interest.[18]

7.30 By way of another example, Liberty and Article 19, have argued that:

> There are at present few, if any, means by which wrongdoing within [the security and intelligence agencies] can be exposed, and the overall public interest properly assessed. In particular, there is no independent means for balancing the public interest in disclosure against any genuine national security considerations.
>
> Given the view of some ex-security and intelligence services officers that there is "no mechanism for internal dissent" and that members of MI5 have "no confidence in the so-called staff counsellor," a former permanent secretary, whistle-blowing appears to some employees within the security and intelligence services as the only way to draw attention to wrongdoing. But relying on whistleblowing to expose wrongdoing is unsatisfactory and a poor substitute for properly effective structures of accountability, both internal and external.[19]

7.31 A good example of such a disclosure in the domestic context is the expense claims of Members of Parliament that were disclosed to the Daily Telegraph in 2009. These disclosures revealed that the system for claiming expenses was deficient.[20] This led to extensive reform of the system for handling such claims. It was generally accepted that even though disclosure of the expense claims may have constituted a criminal offence, for example under the Data Protection Act 1998, it was nevertheless in the public interest to reveal the problems with the system.[21]

7.32 The argument that is often made is that if an individual cannot make a disclosure to the public in the knowledge that they could plead a defence that the disclosure was in the public interest if prosecuted, then wrongdoing may never be brought to light and may never be rectified. A public interest defence could remedy this by encouraging an individual to make a public disclosure safe in the knowledge that they could plead that the disclosure was in the public interest if prosecuted. Of course, as discussed below, they could have no way of knowing in advance whether a jury would ultimately agree with their assessment that the disclosure was in the public interest. The existence of a public interest defence does not eliminate this risk.

[18] S Palmer, “In the Interests of the State: the Government’s Proposals for Reforming Section 2 of the Official Secrets Act 1911” [1988] *Public Law* 523, p 531.

[19] Liberty and Article 19, *Secrets, Spies and Whistleblowers: Freedom of Expression in the UK* (2000), para 7.3.

[20] For an overview of the issues that arose and an assessment of its historic context see G Little and D Stopforth, “The Legislative Origins of the MPs' Expenses Scandal” (2013) 76(1) *Modern Law Review* 83.

7.33 It is unclear whether the objective of enhancing the accountability of government would be better served by an objective or subjective type of public interest defence. On the one hand, a subjective defence would perhaps encourage more disclosures than an objective defence. An individual might have more confidence of success with a genuine belief defence than with a defence that the disclosure was *in fact* in the public interest. Hence such a person may be more likely to proceed with the disclosure. As a result, a subjective defence may reveal more cases of illegality of impropriety than an objective defence.

7.34 On the other hand, a subjective public interest defence may result in protecting unauthorised disclosures that are not in fact in the public interest because they do not reveal sufficiently serious cases of illegality or impropriety. Under such circumstances, individuals would still be absolved of criminal liability if they could demonstrate that their belief was genuine. Such disclosures are difficult to justify by appealing to the need to improve government's accountability.

7.35 An objective version of the defence would avoid this particular problem by protecting only disclosures that are in fact in the public interest. As we have explained, however, the objective version of the defence may not necessarily offer the discloser of the information much protection from criminal liability. Indeed it is speculative and would depend entirely upon the jury's assessment.

PROTECTING THE DISCLOSER OF THE INFORMATION

7.36 A further justification that is often given for why a public interest defence ought to be introduced is the idea that those who make disclosures they believe to be in the public interest should be offered legal protection. Rather than emphasising the importance of the disclosure to the public for the purposes of accountability, this rationale emphasises the benefits of the defence for the individual who wants to make a disclosure in good faith. The rationale underlying this justification seems to be that individuals making unauthorised disclosures in the belief that they are in the public interest should not be criminalised because they do not have the required culpability for criminalisation. Put simply, such individuals meant well.

7.37 Accordingly, this justification only applies to the subjective version of the public interest defence. With the objective version of the defence, the defendant could be convicted even if they believed the disclosure to be in the public interest if the jury disagreed. When considering the subjective version of the defence, however, an individual who genuinely believed the disclosure to be in the public interest would escape criminal liability provided that their belief was genuinely held. It would be for the jury to decide this issue. According to both the objective and subjective formulations of the statutory public interest defence, however, an individual could never be guaranteed protection from criminal liability.

[21] There was no offence contrary to the Official Secrets Act 1989 because the information is question was not encompassed by the legislation.

Problems associated with the introduction of a statutory public interest defence

7.38 We have discussed two justifications for the introduction of a public interest defence in a statutory regime criminalising the disclosure of protected information. Our research also suggests, however, that there are a number of problems associated with the introduction of the defence. The specific problems are:

(1) Undermining the relationship of trust between Ministers and the Civil Service.

(2) The potential risk to others and to national security.

(3) Undermining the principle of legal certainty.

UNDERMINING THE RELATIONSHIP OF TRUST BETWEEN MINISTERS AND CIVIL SERVANTS

7.39 Civil servants must fulfil their role impartially. Impartiality is set out as a core value in the Civil Service Code.[22] If the criminal law condoned the actions of a civil servant who made an unauthorised disclosure of information because they believed that doing so was in the public interest, then this core value could be undermined.

7.40 Allowing such individuals to plead a defence would permit civil servants to weigh government policy against other values when deciding whether or not to comply with their legal obligations. The fundamental reason why civil servants must remain impartial is to "retain the confidence of ministers".[23] Disclosures of sensitive information falling within the categories considered in this paper have the potential to erode this confidence. The Public Accounts Select Committee described this problem in the following terms:

> There is a strong public interest in a Civil Service which is able to act impartially to support the government of the day. Leaks by civil servants undermine the trust that is necessary to this relationship. Leaks for partisan political reasons are especially deplorable. The Civil Service Code is clear that information should not be disclosed without authorisation and the leaking of information by civil servants for political purposes, to undermine government policy or for personal gain, is reprehensible.[24]

7.41 A similar observation was made by the Canadian Supreme Court in the case of *Fraser v Public Service Staff Relations Board*. Delivering the judgment of a

[22] *The Civil Service Code* (2015).

[23] *The Civil Service Code* (2015).

[24] Public Accounts Select Committee, *Leaks and Whistleblowing in Whitehall* (Tenth Report of Session 2008-2009, 2009), para 24. The Committee also concluded that the "right balance" on public interest leaking is set in the Public Interest Disclosure Act 1998. As explained above, the 1998 Act does not encompass disclosures which would constitute a criminal offence. This indicates support for the argument presented here that any further widening of what can be disclosed, through the introduction of a public interest defence, could undermine the impartiality of the civil service.

unanimous Supreme Court, Chief Justice Dickson stated that restrictions on the free speech of public sector employees under the Canadian Charter of Rights and Freedoms could be justified on the basis that the fundamental task of government is to administer and implement policy. In order to do this well, public servants must demonstrate not only knowledge, fairness, and integrity; but also loyalty.[25]

7.42 Maintaining confidence is particularly important in the context of the security and intelligence agencies. This point has been made by Lord Nicholls in the following terms:

> It is of paramount importance that members of the service should have complete confidence in all their dealings with each other, and that those recruited as informers should have the like confidence. Undermining the willingness of prospective informers to co-operate with the services, or undermining the morale and trust between members of the services when engaged on secret and dangerous operations, would jeopardise the effectiveness of the service. An absolute rule against disclosure, visible to all, makes good sense.[26]

POTENTIAL RISK TO OTHERS AND TO NATIONAL SECURITY

7.43 A defence that allows individuals to disclose information because they believe doing so is in the public interest has the potential to pose a risk to others and to national security. Indeed, an individual may conclude that it is in the public interest to disclose information that could have deleterious consequences for others and to national security. They may do so willingly – where they assess the risk to the individual and national security to be outweighed by other considerations – or unwittingly – where they are genuinely unaware of the possible consequences of the disclosure.

7.44 In relation to the latter, an individual will rarely be able to predict the consequences of disclosing the information in question. This is because it should not be assumed that someone who intends to make a disclosure that they believe to be in the public interest will have access to all relevant information when making this determination. The disclosure of information could have unintended consequences. Sir David Omand, for example, has explained this point in the following terms:

> I still would rather the individual civil servant took advice, partly to ensure that they really had all the picture explained to them, which they may very well not have if they are only seeing part of the correspondence. I would rather they took advice.[27]

7.45 Lord Hope made a similar observation in *Shayler.* He stated that:

[25] *Fraser v Public Service Staff Relations Board* [1985] 2 SCR 455 at [41].

[26] *Attorney General v Blake* [2001] 1 AC 286, at 287.

[27] Public Accounts Select Committee, *Leaks and Whistleblowing in Whitehall* (Tenth Report of Session 2008-2009, 2009) paras 18-20 and evidence 18 Question 140 and answer.

> However well-intentioned he or she may be, a member or former member of the security or intelligence services may not be equipped with sufficient information to understand the potential impact of any disclosure. It may cause far more damage than the person making the disclosure was ever in a position to anticipate.[28]

7.46 Beyond not having the full picture themselves, such an individual may fail to appreciate the fact that the information they disclose could be combined with other information so as to jeopardise the safety and security of others or potentially national security. In the national security context, this is commonly referred to as "the mosaic theory". It has been described by Pozen as follows:

> Disparate items of information, though individually of limited or no utility to their possessor, can take on added significance when combined with other items of information.[29]

7.47 By way of example, Pozen cites reports suggesting that information released during the trial of those responsible for the attempted bombing of the World Trade Centre in 1993 was of value to those who committed the 9/11 terrorist attacks.[30] More precisely, it has been suggested that the trial revealed information about the security and intelligence agencies' techniques for tracking suspected terrorists and the force that would be necessary to destroy the Twin Towers.

7.48 Given the fragmented nature of information, it may similarly be impossible for an individual who seeks to disclose information that falls within a protected category to know whether doing so could have damaging consequences.

7.49 It is important to point out that the potential risk to others and to national security is arguably more acute with the subjective version of the defence than with the objective version. This is because the subjective version would allow individuals who unintentionally endanger others by disclosing information to rely on the defence so long as they genuinely believe the disclosure to be in the public interest. By contrast, the objective version of the defence would not be able to be pleaded successfully if the endangering of others outweighed other considerations. Hence with the objective version of the defence, individuals considering whether to disclose information and then subsequently rely on the defence are perhaps less likely to do so.

UNDERMINING LEGAL CERTAINTY

7.50 The introduction of a statutory public interest defence risks undermining the certainty and coherence of the criminal law. In practice, it would be difficult to predict how the defence would operate and when it would be successful or unsuccessful. This uncertainty derives from both the ambivalence of the concept of public interest and the multiple non-legal (moral, political, social, economic)

[28] *R v Shayler* [2002] UKHL 11; [2003] 1 AC 247, para 84.

[29] D Pozen, "The Mosaic Theory, National Security, and the Freedom of Information Act" (2005) 115 *Yale Law Journal* 628, 630.

[30] D Pozen, "The Mosaic Theory, National Security, and the Freedom of Information Act" (2005) 115 *Yale Law Journal* 628, 650 and 678.

reasons that could be advanced to support claims that the unauthorised disclosure in question was (or was not) in the public interest.

7.51 Regarding the inherently ambiguous nature of the concept of public interest, it has been suggested that public interest can be defined in two different and inconsistent ways.[31] First, the public interest may refer to the interests that all members of the public have in common and in equal measure: for instance, the interest in having an effective and accountable government. Secondly, it may refer to the interests of members of the public that are generally served by the government, but which citizens may have in different measures. For instance, an interest in an education system, in a pension scheme and in an effective transport system. Further, it is difficult to distinguish the public interest from similar concepts, such as the national interest.

7.52 It follows that it would be difficult to distinguish between disclosures that serve the public interest from disclosures that do not. Juries would be faced with an impossible task, given that the meaning of public interest is elusive. This means that the understanding of the concept held by the defendant and the jury respectively may diverge. (The same is true of the understandings of different jurors and juries). In addition, the moral and political considerations potentially supporting a public interest defence relate to matters on which individuals may reasonably disagree. This makes it particularly difficult for individuals considering whether to disclose information to know what a jury would conclude. The defence may therefore afford the discloser of the information little legal protection.

7.53 In addition, different juries could arrive at different conclusions on the same set of facts. The possibility that two different juries could arrive at different conclusions regarding what is in the public interest demonstrates the amorphous nature of the concept. Further, such a result would undermine confidence in the justice system and in the ability to protect official data effectively.

7.54 By way of example, a question arose in Denmark as to whether it was in the public interest to disclose classified intelligence information on the alleged weapons of mass destruction programme in Iraq prior to the invasion that occurred in 2003. This issue arose as a result of unauthorised disclosures made by a Danish intelligence officer. The Eastern High Court of Denmark did not consider that the unauthorised disclosure was made in "the obvious public interest" because it did not reveal any illegal activity or wrongdoing. The Copenhagen City Court, however, ruled otherwise solely on the grounds that there was considerable public interest in knowing the basis for the decision that was taken to involve Denmark in the invasion of Iraq.[32]

7.55 Turning to the non-legal considerations that could be advanced to support a public interest defence, these encompass moral, political, social, economic issues in addition to consideration of the motives of the defendant. With the objective version of the defence, non-legal considerations would be advanced to argue that a disclosure was in fact in the public interest. With the subjective

[31] For discussion, see J Horder, *Ashworth's Principles of Criminal Law* (8th edn 2016), pp 47 – 50.

[32] For discussion, see H Nasu, "State secrets and national security" (2015) *International and Comparative Law Quarterly* 365, 395.

version of the defence, evidence of the defendant's motives would be adduced to demonstrate that they genuinely (or reasonably) believe the disclosure to be in the public interest.

7.56 Typically, however, the criminal law excludes such considerations. The criminal law prohibits conduct that is judged to be harmful and wrongful by society notwithstanding the non-legal justifications and individual motivations that might exist for engaging in such conduct. This is the case even in what some might regard as more acute scenarios. For example, in *Inglis* the Lord Chief Justice explained that although an individual who kills a loved one in order to end their suffering, so-called "mercy killing", may have good motives, the law still condemns this act as murder.[33] As was explained in the White Paper that preceded the Official Secrets Act 1989:

> The Government recognises that some people who make unauthorised disclosures do so for what they themselves see as altruistic reasons and without desire for personal gain. But that is equally true of some people who commit other criminal offences. The general principle which the law follows is that the criminality of what people do ought not to depend on their ultimate motives − though these may be a factor to be taken into account in sentencing − but on the nature and degree of the harm which their acts may cause.[34]

7.57 Introducing such considerations into a jury's determination of whether a criminal offence has been proved would undermine the coherence of the criminal law and thereby create uncertainty.

7.58 Similar arguments have been invoked to criticise the existence of a general defence of necessity. For example Norrie has argued that the defence "operates to permit alternative political, ethical, economic and moral arguments to confront the formal logic of the law".[35] The analogy with necessity is particularly relevant in that both defences seek to permit conduct that is unlawful on the basis that engaging in the unlawful conduct will avoid an even greater harm.

7.59 The inherently uncertain nature of a public interest defence also has the potential to impact upon the criminal justice system as a whole, in a number of ways.

7.60 First, the uncertainty of the defence could undermine principles that are key to the criminal justice system. For example, currently the Code for Crown Prosecutors mandates that prosecutors must consider whether prosecution is required in the public interest.[36] In doing so, they have to consider the seriousness of the offence, the culpability of the suspect, the harm to the victim, and the impact on the community, among other factors. If a public interest defence was created, the question of whether a prosecution is in the public interest and whether the disclosure was in the public interest may become conflated. As a result, the number of prosecutions for unauthorised disclosures

[33] *R v Inglis* [2010] EWCA Crim 2637; [2011] 1 WLR 1110.

[34] Reform of Section 2 of the Official Secrets Act 1911 (1988) Cm 408, para 59.

[35] A Norrie, *Crime, Reason and History* (3rd ed 2014), pp 217-218.

[36] Crown Prosecution Service, *Code for Crown Prosecutors* (January 2013), p 7.

may increase: prosecutors may reason that the public interest question should be left to the jury in cases of unauthorised disclosures.

7.61 For instance, in 2011 in the context of operation Elveden, nine of the resulting prosecutions were discontinued after a reassessment of the public interest question by the then Director of Public Prosecutions. Operation Elveden involved a number of governmental officials who had disclosed confidential information to journalists. The reasoning beyond discontinuing prosecution involved consideration of whether the disclosures were in the public interest or on the contrary were detrimental to it.[37] Had a public interest defence been available, the proceedings may have been continued and the question addressed to the jury.

7.62 Related to this problem, the introduction of a public interest defence could have the effect of transferring the question of public interest from the prosecutor to the jury, thereby causing the defendant to lose the protection afforded by the public interest stage of the Code for Crown Prosecutors.[38] Indeed, it has been argued that including a statutory public interest defence for offences contained in the Official State Secrets Act 1989 is unnecessary because the public interest is already considered by the Attorney General when deciding whether to prosecute.[39] This requirement was described by Lord Bingham in *Shayler* as providing an effective safeguard, as the Attorney General may take a broader view of the public interest and is not simply confined to CPS guidance.[40] Furthermore, it is not obvious that a jury would be predisposed to be more sympathetic than a prosecutor towards someone who discloses information contrary to the criminal law.

7.63 Secondly, the lack of clarity surrounding the concept of public interest would open the floodgates: virtually *anyone* who wishes to raise the defence in relation to a charge of unauthorised disclosure could do so, notwithstanding the circumstances in which the offence was committed. If public interest was a defence to unauthorised disclosure, it seems that no information could necessarily ever be guaranteed to be safe.

7.64 In conclusion, a public interest defence risks creating legal uncertainty and has the potential to undermine the efficiency of the criminal justice system. Arguably, some of the problems identified could be mitigated through careful legislative drafting. For instance, a statutory defence could be accompanied by a non-exhaustive list of factors to be taken into consideration (by prospective disclosers, juries, practitioners) when assessing whether a disclosure is in the public interest. A list of examples could also be included in the explanatory note for the bill. These factors and examples could then be included in jury directions. The

[37] http://www.cps.gov.uk/news/latest_news/crown_prosecution_service_re_review_of_operation_elveden/ (last visited 10 November 2016).

[38] The Full Code test for the Code for Crown Prosecutors has two stages: (i) the evidential stage; followed by (ii) the public interest stage. Available at: https://www.cps.gov.uk/publications/code_for_crown_prosecutors/codetest.html (last visited 10 November 2016).

[39] P Birkinshaw and M Varney, *Government and Information: The Law Relating to Access, Disclosure and their Regulation* (4th ed 2011), p 234.

[40] *R v Shayler* [2002] UKHL 11; [2003] 1 AC 247, para 35-36.

problems identified in this section, however, also impede legislative drafting itself: the factors defining the public interest would be particularly difficult to select and unavoidably contentious.

Conclusion on the introduction of a statutory public interest defence

7.65 We have provisionally concluded that the problems associated with the introduction of a statutory public interest defence outweigh the benefits. Of particular relevance in arriving at this provisional conclusion is our belief that the public interest can be better served by the introduction of the statutory commissioner model, which we examine later in this chapter.

Provisional conclusion 23

7.66 **The problems associated with the introduction of a statutory public interest defence outweigh the benefits. Do consultees agree?**

A statutory public interest defence for journalistic activity

7.67 We accept that different considerations may apply in the context of journalistic activity given that the press "plays a vital function in democracy".[41] In his *Inquiry into the Culture, Practices and Ethics of the Press*, Lord Justice Leveson doubted whether journalists ought to be treated differently from other citizens for the purposes of determining whether they have committed criminal offences.[42] After accepting the importance of a free press, Lord Justice Leveson commented:

> In a modern democracy that abides by the rule of law, press freedom can never mean a press which sits outside, above and beyond, or in disregard of, the law. Respect for the law is the common framework within which the press, as an important commercial sector, is enabled to flourish, to preserve and enjoy its freedoms, and to make its unique contribution to a democratic society.[43]

7.68 Lord Justice Leveson added that:

> A press considering itself to be above the law would be a profoundly anti-democratic press, arrogating to itself powers and immunities from accountability which would be incompatible with a free society more generally.[44]

7.69 Lord Justice Leveson later considered two practical issues associated with the introduction of a statutory public interest defence specifically for journalists.

[41] B Leveson, *An Inquiry into the Culture, Practices and Ethics of the Press* (2012), Vol 1, Ch 2, para 5.1.

[42] B Leveson, *An Inquiry into the Culture, Practices and Ethics of the Press* (2012), Vol 1, Ch 2, para 5.6.

[43] B Leveson, *An Inquiry into the Culture, Practices and Ethics of the Press* (2012), Vol 1, Ch 2, para 5.5.

[44] B Leveson, *An Inquiry into the Culture, Practices and Ethics of the Press* (2012), Vol 1, Ch 2, para 5.6.

7.70 First, such a defence could preclude the commencement of a prosecution even when the activity in question was clearly not in the public interest. Lord Justice Leveson elaborated as follows:

> [H]ow could the proposed [public interest] defence to an allegation of bribery or blackmail ever be tested? The journalist will say (whether honestly or not) that the information came from a reliable source, responsible in the past for much entirely accurate material, whom he is not prepared to name under any circumstances. The effect of a defence in law will be to emasculate almost all prospect of bringing a journalist to task for the way in which a story has been researched, whatever means, at first blush illegal, might have been used.[45]

7.71 By way of context, Lord Justice Leveson had earlier examined journalists' use of questionable means, including procuring unauthorised disclosures from various individuals, to secure information for articles in which there was little or no public interest.[46]

7.72 Secondly, Lord Justice Leveson queried the necessity of introducing a public interest defence specifically for journalists. Given the fact the Director of Public Prosecutions has promulgated guidelines that must be considered when a prosecutor is deciding whether to charge a journalist with a criminal offence, Lord Justice Leveson concluded that sufficient safeguards were already in place. These guidelines set out the approach that prosecutors should take when making decisions where they affect the media and, in particular, how prosecutors should approach the question of whether a prosecution is required in the public interest. The guidelines are drafted to ensure compliance with Article 10 of the European Convention on Human Rights.

7.73 In this regard, Lord Justice Leveson also cited the safeguards that apply throughout the criminal law more generally.[47] These safeguards consisted of the judge's discretion to advise prosecuting counsel on the need to take further instruction from the prosecuting authority on whether to proceed with the prosecution, the power to stay proceedings as an abuse of process, jury (in)equity, and the "ultimate safeguard" of the discretion of the judge when sentencing.

7.74 For the reasons identified above and given the depth and breadth of analysis in such a recent report, we agree with Lord Justice Leveson's conclusion that journalistic activity is already sufficiently protected by the safeguards that currently exist. The guidelines promulgated by the Director of Public Prosecutions are designed to ensure that a journalist is only prosecuted when this is clearly in the public interest. Even in the absence of a statutory public interest defence, there are safeguards in place to ensure that journalists are not prosecuted routinely.

[45] B Leveson, *An Inquiry into the Culture, Practices and Ethics of the Press* (2012), Vol 4, Ch 2, para 6.6.

[46] B Leveson, *An Inquiry into the Culture, Practices and Ethics of the Press* (2012), Vol 2, Ch 2, para 3.58-3.77.

[47] B Leveson, *An Inquiry into the Culture, Practices and Ethics of the Press* (2012), Vol 4, Ch 2, paras 7.1 – 9.

7.75 In addition, it is our view that the introduction of a statutory public interest defence solely for journalists could be considered arbitrary, given that there are other professionals who might violate the criminal law in the pursuit of their legitimate activities.

Provisional conclusion 24

7.76 **The legal safeguards that currently exist are sufficient to protect journalistic activity without the need for a statutory public interest defence. Do consultees agree?**

Model 2: The statutory commissioner model

7.77 Although we have provisionally concluded that the case has not been made for the introduction of a statutory public interest defence, we do believe there are other models that would ensure alleged illegality or impropriety can be brought to light without the problems associated with such a defence. We believe such mechanisms are central to addressing the concerns raised by those who argue that there ought to be a public interest defence to enable alleged illegality or impropriety to be addressed.

7.78 In this section we examine the extent to which such processes exist within the current law and evaluate whether improvements could be made. It is necessary to draw a distinction between Crown servants generally and members of the security and intelligence agencies. For the sake of clarity, these respective categories will be considered separately.

The position of civil servants generally

7.79 All civil servants are bound by the Civil Service Code, which contains the following guidance for those who have concerns about alleged illegality or impropriety:

> Your department or agency has a duty to make you aware of this Code and its values. If you believe that you are being required to act in a way which conflicts with this Code, your department or agency must consider your concern, and make sure that you are not penalised for raising it.
>
> If you have a concern, you should start by talking to your line manager or someone else in your line management chain. If for any reason you would find this difficult, you should raise the matter with your department's nominated officers who have been appointed to advise staff on the code.
>
> If you become aware of actions by others which you believe conflict with this code you should report this to your line manager or someone else in your line management chain; alternatively you may wish to seek advice from your nominated officer. You should report evidence of criminal or unlawful activity to the police or other appropriate

regulatory authorities. This code does not cover HR management issues.[48]

7.80 If a civil servant is not satisfied with the response he or she receives after following this process, they may report the matter in question to the Civil Service Commission. The Civil Service Commission was placed upon a statutory footing by section 1 of the Constitutional Reform and Governance Act 2010. By virtue of section 9(2) of the Constitutional Reform and Governance Act 2010, a civil servant may complain to the Civil Service Commission if:

(1) they are being, or have been, required to act in a way that conflicts with the code, or

(2) another civil servant covered by the code is acting, or has acted, in a way that conflicts with the code.

7.81 The Civil Service Commission has statutory powers that enable it to investigate complaints. For example, by virtue of section 9(6) of the Constitutional Reform and Governance Act 2010, for the purposes of the investigation or consideration of a complaint, the following *must* provide the Commission with any information it reasonably requires:

(1) civil service management authorities;

(2) the complainant; and

(3) any civil servant whose conduct is covered by the complaint.

7.82 In its 2014-2015 Annual Report, the Commission stated that its aim is to acknowledge complaints within three working days and to complete initial assessments on whether a case is in scope within 15 working days.[49] Following an investigation, the Commission will send a report of its findings to the individual complainant and the department concerned. The Civil Service Commission then has the power to make recommendations about how the matter in question ought to be resolved. Although there is no legal obligation to follow these recommendations, the Commission suggests that if its recommendations are ignored, it can bring public and parliamentary attention to this fact and raise the matter with the Permanent Secretary of the department in question and the Cabinet Secretary, if necessary. There is no way to appeal against a decision that has been taken by the Civil Service Commission.[50]

7.83 According to research conducted by Savage, the total number of approaches civil servants have made to the Civil Service Commission has remained low since it gained the power to investigate.[51] For example, between March 2014 and April

[48] *Civil Service Code,* Available at: https://www.gov.uk/government/publications/civil-service-code/the-civil-service-code (last accessed: 10 November 2016).

[49] Annual Report and Accounts 2014-2015, Report of the Civil Service Commission (2015) HC 251, p 44.

[50] For further discussion, see A Savage, *Leaks, Whistleblowing and the Public Interest* (2016), pp 187 – 191.

[51] A Savage, *Leaks, Whistleblowing and the Public Interest* (2016), p 187.

2015, the Commission dealt with four cases.[52] Savage attributes these low figures to two factors.[53] First, many of the complaints made to the Commission concern human resource issues which it rejects on the basis that the Civil Service Code precludes it from considering such matters. Secondly, Savage suggests that the Commission's own guidance steers prospective complainants towards internal departmental and agency complaint mechanisms. We would welcome views from consultees on the effectiveness of the Civil Service Commission as a mechanism for receiving unauthorised disclosures.

Consultation question 15

7.84 **We welcome views from consultees on the effectiveness of the Civil Service Commission as a mechanism for receiving unauthorised disclosures.**

7.85 Although it is used infrequently, something which is perhaps attributable to its own guidance, a process does exist that enables concerns from civil servants to be investigated by independent statutory commissioners. We believe that this satisfies the public interest as it means allegations of impropriety can be investigated and ultimately resolved.

7.86 The next section will consider the extent to which such a process is available to members of the security and intelligence agencies.

Members of the security and intelligence agencies

7.87 Given the sensitive nature of their work, a different regime operates for members of the security and intelligence agencies who wish to raise a concern that relates to their employment. As the House of Lords in *Shayler* explained, there is a list of officeholders who can be approached directly with any concerns, such as the Attorney General and the Commissioner of the Metropolitan Police Service.[54] Lord Bingham explained that:

> These officers are subject to a clear duty, in the public interest, to uphold the law, investigate alleged infractions and prosecute where offences appear to have been committed, irrespective of any party affiliation or service loyalty.[55]

7.88 In addition to these officeholders, there are a number of processes which exist and which are available to a member of the security and intelligence agencies who has concerns relating to their work. A tiered regime is in operation, in the sense that concerns are first raised internally but then can also be raised with someone who is independent of the agency in question.

[52] Annual Report and Accounts 2014-2015, Report of the Civil Service Commission (2015) HC 251, pp 43 – 44.

[53] A Savage, *Leaks, Whistleblowing and the Public Interest* (2016), pp 187 – 188.

[54] *R v Shayler* [2002] UKHL 11; [2003] 1 AC 247, para 27. The Attorney General and the Commissioner of the Metropolitan Police Service are included as persons to whom authorised disclosures can be made in the Official Secrets Act (Prescription Order) 1990, SI 1990/200.

[55] *R v Shayler* [2002] UKHL 11; [2003] 1 AC 247, para 27.

7.89 First, as the Intelligence and Security Committee of Parliament noted in its 2007-2008 Annual Report, in 2006 the Security Service established the post of "Ethical Counsellor". The Intelligence and Security Committee described the work of this post in the following terms:

> To provide staff with an internal avenue to raise any ethical concerns they may have about the Service's work with someone who is outside their management line.[56]

7.90 The Committee noted that this post was held by a "former Deputy Director General of the Service", but did not provide any further details. For example, the Intelligence and Security Committee did not clarify whether a similar post existed in the other security and intelligence agencies or whether it was confined to the Security Service. In addition, Savage states that it is not clear whether this post still exists.[57] Stakeholders have confirmed to us, however, that this post is still in existence and that each of the security and intelligence agencies has its own Ethical Counsellor.

7.91 Secondly, if the individual in question wishes to raise the matter with someone who is independent of the agency in question, then they can contact the Staff Counsellor. The post of Staff Counsellor was established in 1987 by the then Prime Minister Margaret Thatcher. The Prime Minister described the role in the following terms:

> He will be available to be consulted by any member of the security and intelligence services who has anxieties relating to the work of his or her service which it has not been possible to allay through the ordinary processes of management-staff relations. He will have access to all relevant documents and to any level of management in each service. He will be able to make recommendations to the head of the service concerned. He will also have access to the Secretary of the Cabinet if he wishes and will have the right to make recommendations to him. He will report as appropriate to the heads of the services and will report not less frequently than once a year to me and to my Right Hon. friends the Foreign and Commonwealth Secretary and the Home Secretary as appropriate on his activities and on the working of the system.[58]

7.92 The post of Staff Counsellor is fulfilled by someone who is not a member of any of the security and intelligence agencies. If a member of the security and intelligence agencies has raised their concern with someone within the agency in question but is dissatisfied with the response they have received, the existence of the Staff Counsellor ensures that the matter can be brought to the attention of someone who is independent of the agency in question.

7.93 Following David Shayler's unauthorised disclosure of classified documents to a newspaper, the Intelligence and Security Committee took evidence from the then

[56] Intelligence and Security Committee, 2007-2008 Annual Report (March 2008) Cm 7542, para 66.

[57] A Savage, *Leaks, Whistleblowing and the Public Interest* (2016), p 210.

[58] Written Answer, Hansard (HC), 2 November 1987, vol 121, col 508W.

Staff Counsellor, Sir Christopher France. Sir Christopher reported that he and his predecessors had handled approximately 149 cases since the role of Staff Counsellor was created in 1987.[59]

7.94 The role of the Staff Counsellor has been criticised on a number of occasions. For example, Machon has suggested that the role is "seen as a joke" by those intended to rely upon it.[60] Katharine Gun stated that she chose not to approach the Staff Counsellor before leaking documents to the Guardian because she felt that the matter was "so urgent it needed direct action" and that she believed that the person would "probably say "well, we appreciate your concerns, we'll take it into consideration and perhaps we should meet in a week or so" [which] was not going to be adequate".[61]

7.95 Contrary to these criticisms, stakeholders emphasised to us during our preliminary consultation that there is confidence in the role performed by the Staff Counsellor. The Staff Counsellor is perceived to be a relatively informal means of addressing concerns through dialogue and explanation.

7.96 Although we are confident that the role performed by the Staff Counsellor is valuable and ought to be retained, we nevertheless believe it is necessary to evaluate whether more formal means ought to exist that would enable a member of the security and intelligence agencies to bring a concern relating to their work to the attention of a statutory officeholder who is independent of the agency in question. This would add an additional, external tier to the regime that is currently in operation.

Options for the introduction of a statutory post

7.97 This section of the chapter will evaluate two options for adding an additional, external tier to the regime that is currently in operation.

7.98 Ideally, any statutory post established for these purposes would broadly have the same characteristics and powers as the Civil Service Commissioners, subject to any changes that might be necessary to reflect the sensitive nature of the work undertaken by the security and intelligence agencies. This would ensure civil servants generally and members of the security and intelligence agencies have similar processes available to them. These characteristics and powers are as follows:

(1) The concern is disclosed to someone who holds a statutory appointment.

(2) This officeholder has security of tenure.

[59] The Intelligence and Security Committee's Annual Report (1998) Cm 4073, para 36. For analysis see A Savage, *Leaks Whistleblowing and the Public Interest* (2016), pp 208 - 209.

[60] A Machon, *Spies, Lies and Whistleblowers* (2005), p 109.

[61] Anon, "GCHQ: it was full of people like me" (*Gloucester Echo,* 27 October 2004). Katherine Gun was employed at the Government Communication Headquarters who was charged with committing offences contrary to the Official Secrets Act 1989 after she disclosed information to a newspaper concerning surveillance requests received from the United States in the build up to the 2003 invasion of Iraq.

(3) There is a specified timeframe within which the officeholder must address the complaint.

(4) The officeholder has the ability to investigate matters that are brought to his or her attention and there is a statutory obligation placed upon the relevant parties to assist the investigation.

(5) The officeholder has an obligation to report to government, with an obligation for that report to be laid before Parliament, subject to the need to ensure information relating to national security is not jeopardised.

7.99 We believe there are two possible ways these aims could be achieved. These will be outlined in the following sections.

ENSHRINE THE POST OF STAFF COUNSELLOR IN LEGISLATION

7.100 One option is to enshrine in legislation the mechanism that already exists, namely the Staff Counsellor. This could also provide an opportunity to clarify the nature of the role played by the Staff Counsellor, specify in detail the post holder's powers, and bring a greater degree of transparency to the appointment process.

7.101 Although this option would be the simplest in terms of implementation, we believe it is not the best solution for two reasons. First, it would not constitute a substantive change from the regime that currently exists and would not bring the benefits associated with the creation of an additional, external officeholder who would have the power formally to investigate a concern. Secondly, it could undermine the Staff Counsellor's role as an informal, independent mediator who achieves the resolution of issues by way of dialogue and explanation. For these reasons, we believe it is necessary to consider whether an additional post ought to be created that would complement the function performed by the Staff Counsellor.

RETAIN THE ROLE OF STAFF COUNSELLOR AND ESTABLISH A STATUTORY COMMISSIONER

7.102 A second option is to retain the post of Staff Counsellor and establish a statutory commissioner who could receive and investigate concerns from members of the security and intelligence agencies. These posts would be complementary in the sense that the Staff Counsellor would continue to act as a more informal mediator whilst the statutory commissioner would be available if a member of staff wished to invoke a more formal process.

7.103 There are currently a number of statutory offices in existence that could be relied upon as a template for the creation of such a statutory commissioner. These include the Intelligence Services Commissioner and the Interception of Communications Commissioner.

7.104 At this stage it is important to point out that the Investigatory Powers Act 2016 will, once the relevant provisions come into force, abolish these various statutory offices and replace them with the Investigatory Powers Commissioner who is supported by a number of Judicial Commissioners.

7.105 The role the Investigatory Powers Commissioner is intended to play is detailed in Part 8 of the Investigatory Powers Act 2016, specifically in sections 227 – 240.

This part of the Act is entitled *Oversight Arrangements.* The Act mandates that the Prime Minister must appoint the Investigatory Powers Commissioner and a number of Judicial Commissioners. Section 227 mandates that a Judicial Commissioner must hold or have held a high judicial office. They are appointed for a term of three years initially, may be reappointed and cannot be removed from office before the end of their term unless a resolution approving the removal has been passed by each House of Parliament.

7.106 The main oversight functions of the Investigatory Powers Commissioner are set out in section 229 of the Investigatory Powers Act. The Act specifies what the Investigatory Powers Commissioners must keep under review (including by way of audit, inspection and investigation).

7.107 The Act contains provisions that detail the nature of the role played by the Investigatory Powers Commissioner. The Investigatory Powers Commissioner has powers that allow him or her to investigate. Section 235 mandates that "Every relevant person must disclose or provide to a Judicial Commissioner all such documents and information as the Commissioner may require for the purposes of the Commissioner's functions."

7.108 In addition, by virtue of section 236, the Intelligence and Security Committee of Parliament can refer a matter to the Investigatory Powers Commissioner with a view to the Commissioner carrying out an investigation, inspection or audit into it. This ensures that there will be interaction between the Investigatory Powers Commissioner and Parliament.

7.109 In order to ensure that the work of the Investigatory Powers Commissioner is transparent, section 234 states that he or she must report to the Prime Minister about the carrying out of the functions of the Commissioners. The Act imposes upon the Prime Minister a duty to publish the report and lay a copy before Parliament.

7.110 Of particular relevance to this paper, section 237 contains what is entitled the "Information gateway". This clause is set out below:

> (1) A disclosure of information to the Investigatory Powers Commissioner or another Judicial Commissioner for the purposes of any function of the Commissioner does not breach—
>
> (a) an obligation of confidence owed by the person making the disclosure, or
>
> (b) any other restriction on the disclosure of information (whether imposed by virtue of this Act or otherwise).
>
> (2) But subsection (1) does not apply to a disclosure, in contravention of any provisions of the Data Protection Act 1998, of personal data which is not exempt from those provisions.

7.111 The Explanatory Notes to the Act explain how this provision is intended to function in the following terms:

> This clause allows people to provide information to the Investigatory Powers Commissioner, regardless of any other legal restrictions that might exist. This means that, for example, someone whose work relates to the use of investigatory powers may tell a Judicial Commissioner about their work, and any concerns they may have, without being censured for doing so. An exception to this is that the protections in the Data Protection Act 1998 still apply when information is provided to the Investigatory Powers Commissioner.

7.112 This provision therefore enables someone who has concerns about the exercise of investigatory powers, or indeed anything else the Investigatory Powers Commissioner is directed by the Prime Minister to oversee, to bring them to the attention of the Investigatory Powers Commissioner without being censured for doing so.

7.113 We believe that, once the relevant provisions are commenced, the Investigatory Powers Commissioner, supported by the Judicial Commissioners, would provide a suitable means of ensuring that members of the security and intelligence agencies have an additional option available to them should they wish to raise a concern relating to their work in a more formal setting with an officeholder who is independent of the agency in question. That would be an additional function of the Investigatory Powers Commissioner that ought to be made explicit.

7.114 The addition of this more formal process to the regime that currently exists would have the following benefits. First, the Investigatory Powers Commissioner is intended to embody a much greater degree of transparency than the Staff Counsellor, as evidenced by the duty to report. In addition, David Anderson QC, the Independent Reviewer of Terrorism Legislation, stated that the version of the Investigatory Powers Commissioner he recommended ought to be established should be outward-facing, should have name recognition and a public profile.[62] Secondly, there is a statutory obligation to provide the Investigatory Powers Commissioner with any documents or information that are needed for him or her to carry out his or her functions, so pertinent information cannot be withheld. Thirdly, it would ensure that an individual with concerns that relate to their employment in the security and intelligence agencies could raise them without risking prosecution.

7.115 The combination of these factors leads us to conclude that the existence of a robust mechanism addresses the concerns of those who argue that there ought to be a statutory defence that could be pleaded by someone who makes a disclosure they believe to be in the public interest. This is because an individual who has concerns relating to their employment in the security and intelligence agencies would be able to disclose them to a statutory officeholder without committing a criminal offence, that officeholder would be able to investigate the matter, there would be an obligation to cooperate with that investigation and a report detailing the work of the Investigatory Powers Commissioner, which would potentially include details of any investigation, would be laid before Parliament, subject to the need to ensure sensitive information is not jeopardised.

[62] D Anderson, *A Question of Trust – Report of the Investigatory Powers Review* (2015), para 14.94 – 14.100.

Conclusion on the statutory commissioner model

7.116 For the reasons we have given in the previous paragraphs, we believe that the position of Staff Counsellor ought to be retained, but that it ought to be supplemented by the Investigatory Powers Commissioner. That this is an additional function of the Investigatory Powers Commissioner ought to be made explicit. This would mean that a member of the security and intelligence agencies harbouring concerns relating to their work would have the option of not only disclosing this concern internally to the Ethical Counsellor, but also externally to the Staff Counsellor and, if they were still not satisfied, then the issue could be brought to the attention of the Investigatory Powers Commissioner.

7.117 We believe that this three-tiered process would have the benefit of enhancing public confidence in the ability to deal effectively with complaints raised by agency staff and also addresses the concerns of those who express the view that there ought to be a statutory public interest defence. As we pointed out above, in a joint report, Liberty and Article 19 stated that:

> Relying on whistleblowing to expose wrongdoing is unsatisfactory and a poor substitute for properly effective structures of accountability, both internal and external.[63]

7.118 We agree with Liberty and Article 19's conclusion that whistleblowing is a poor substitute for properly effective structures of accountability. It is for this reason that we have sought to enhance the structures that are currently in place.

Provisional conclusion 25

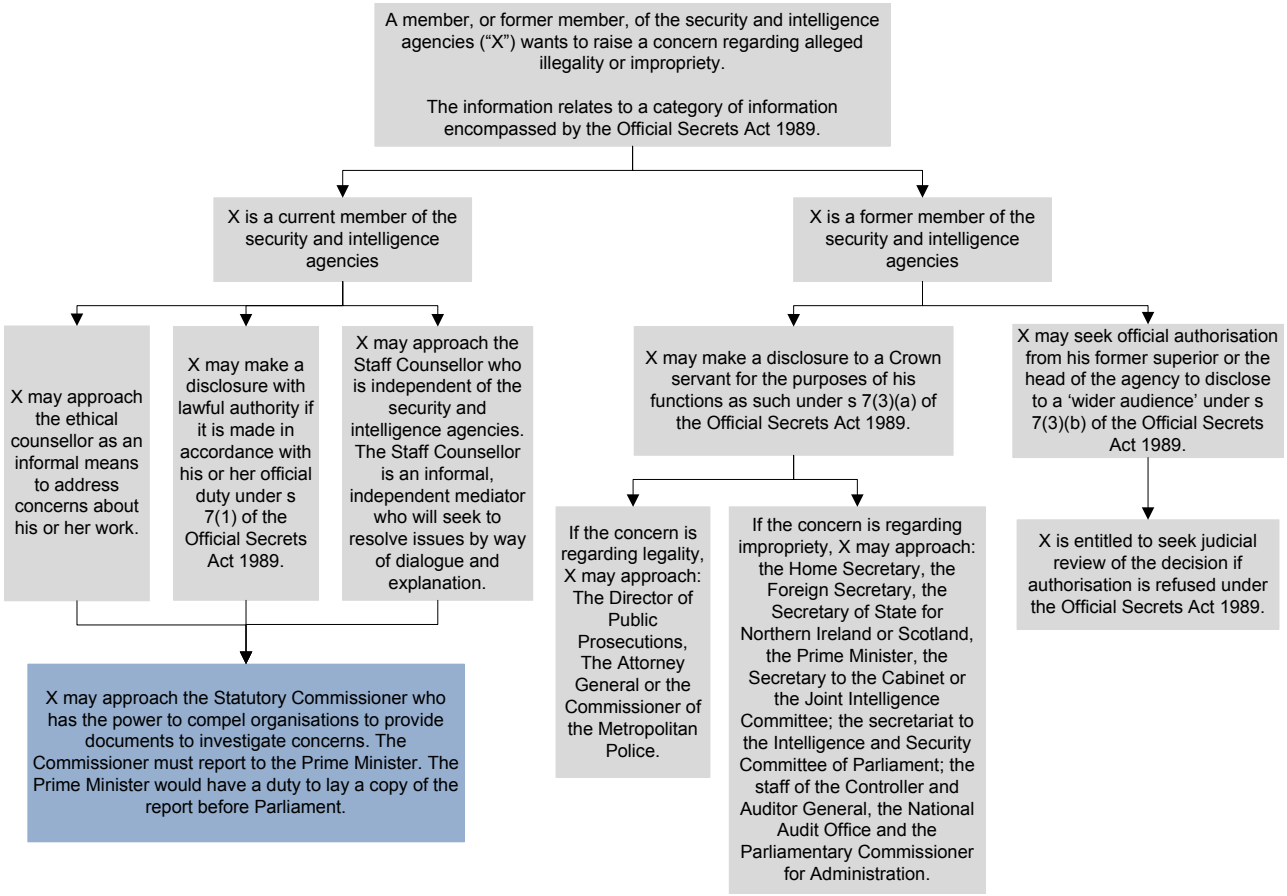
7.119 **A member of the security and intelligence agencies ought to be able to bring a concern that relates to their employment to the attention of the Investigatory Powers Commissioner, who would be able to investigate the matter and report their findings to the Prime Minister. Do consultees agree?**

7.120 Before leaving this issue, it is necessary to clarify that although the discussion in this part of the chapter has focused upon members of the security and intelligence agencies, the Staff Counsellor is available to be consulted by staff in other departments closely involved in intelligence work provided that the issue they wish to discuss relates to their access to intelligence.[64] We envisage the Investigatory Powers Commissioner being available to receive concerns from members of staff in these departments in addition to those working in the security and intelligence agencies. Indeed the explanatory notes to the Investigatory Powers Act 2016 state that the Investigatory Powers Commissioner can be contacted by all bodies with a link to investigatory powers, even if these are private companies rather than public authorities.

7.121 Below we have produced a diagram to illustrate how the Investigatory Powers Commissioner model would fit within the existing framework.

[63] Liberty and Article 19, *Secrets, Spies and Whistleblowers: Freedom of Expression in the UK* (2000), para 7.3.

[64] This was confirmed by the Prime Minister in a written statement to the House of Commons. See Hansard (HC), 21 April 2016, HCWS694, vol 608, cc 27WS – 28WS.



7.122 As can be seen, the statutory commissioner model provides an additional avenue by which to raise concerns and ensures:

(1) Information that may cause damage if it were to be disclosed is protected.

(2) Greater accountability is achieved by the power of the Investigatory Powers Commissioner to investigate matters that are brought to his or her attention. This is augmented by the existence of a statutory obligation to assist any investigation carried out by the commissioner. A degree of transparency is ensured by the obligation to lay a report detailing the work of the statutory commissioners before Parliament.

Model 3: The "Canadian model"

7.123 Our comparative law research has revealed the existence of a third model. In Canadian law the Security of Information Act 2001 makes it a criminal offence for anyone permanently bound to secrecy from communicating or confirming "special operational information". Such an individual does not commit an offence under Act if their purpose is to:

> Disclose an offence under an Act of Parliament that he or she reasonably believes has been, is being, or is about to be committed by another person in the purported performance of that person's duties and functions for, or on behalf of, the Government of Canada.

7.124 In addition, the public interest in disclosure of the information must outweigh the public interest in non-disclosure. The legislation enumerates the factors a court must consider when assessing whether the disclosure was in the public interest.

7.125 If an individual is charged with committing an offence contrary to the Security of Information Act 2001, a court can consider a public interest defence only if he or she followed a series of steps set out in the legislation before disclosing the special operational information. First, the individual must have brought the matter to the attention of the relevant organisation's deputy head or the Deputy Attorney General of Canada. If the individual did not receive a response from the deputy head or the Deputy Attorney General within a reasonable time, then the concern must have been brought to the Communications Security Establishment Commissioner who must have been allowed a reasonable time to respond. Failure to follow this procedure precludes the individual from pleading that the disclosure was in the public interest.

7.126 Despite the fact this mechanism has been in place for a number of years, it has never been relied upon. For that reason, it is difficult to assess its practical merits.

7.127 In addition to this practical difficulty, we are not convinced that this model offers benefits beyond those that would follow from our provisional conclusion that a statutory commissioner ought to be available to receive and investigate complaints. One of the key reasons why we provisionally concluded that complaints ought to be able to be brought to the Investigatory Powers Commissioner is our belief that it ensures the public interest in addressing the concerns of those employed by the security and intelligence agencies is satisfied.

7.128 The introduction of a public interest defence that would be available only if the Investigatory Powers Commissioner failed to address a concern that was brought to his or her attention could have the effect of undermining confidence in the role and might encourage individuals to make anonymous disclosures.

7.129 This model exhibits many of the problems we identified with the statutory public interest defence model, namely:

(1) Undermining the relationship of trust between Ministers and civil servants by allowing civil servants to weigh government policy against other values when deciding whether or not to make an unauthorised disclosure.

(2) The possibility of compounding damage caused by the initial disclosure. One of the factors to be considered under the Security of Information Act 2001 when deciding whether an unauthorised disclosure was in the public interest is the extent of the harm or risk of harm created by the disclosure.[65] The public confirmation that such damage has occurred has the potential to compound the damage caused by the initial unauthorised disclosure.

(3) Undermining the principle of legal certainty. As we discussed above, uncertainty derives from both the ambivalence of the concept of public

[65] Security of Information Act 2001, s 15(4)(f).

interest and the multiple non-legal (moral, political, social, economic) reasons that could be advanced to support claims that the unauthorised disclosure in question was (or was not) in the public interest. For example, another factor to be considered under the Security of Information Act 2001 is "the existence of exigent circumstances justifying the disclosure".[66] This provision theoretically allows a defendant to rely on a multitude of reasons potentially to justify an unauthorised disclosure.

Conclusion on the "Canadian model"

7.130 For the reasons given in the previous paragraphs, we do not believe that the Canadian model would bring additional benefits or overcome a number of the problems caused by the introduction of a statutory public interest defence identified above. Furthermore, the model could undermine confidence in the ability of the Investigatory Powers Commissioner to discharge his or her functions.

Provisional conclusion 26

7.131 **The Canadian model brings no additional benefits beyond those that would follow from there being a statutory commissioner who could receive and investigate complaints from those working in the security and intelligence agencies. Do consultees agree?**

PUBLIC DISCLOSURES

7.132 The mechanism we have provisionally concluded ought to be introduced would enable a member of the security and intelligence agencies to raise a concern relating to their work with an officeholder independent of their organisation.

7.133 This process would not authorise such an individual to make a public disclosure. If they were to make such a disclosure, this may constitute an offence contrary to the Official Secrets Act 1989. Even if it were argued that the disclosure was in the public interest (however defined), this would be no defence. As we have discussed both in this chapter and earlier in Chapter 6 we believe such a defence poses difficulties of principle and is not required by the European Convention on Human Rights.

7.134 In considering the process for making public disclosures, for example by way of publishing a memoir, it is necessary to contrast the position of current Crown servants and members of the security and intelligence agencies, with former Crown servants and former members.

7.135 If a former member of the security and intelligence agencies wishes to make a public disclosure, they would be able to seek official authorisation in accordance with section 7(3) of the Official Secrets Act 1989 and described by Lord Bingham in *Shayler* in the following terms:

> Consideration of a request for authorisation should never be a routine or mechanical process: it should be undertaken bearing in mind the importance attached to the right of free expression and the need for

[66] Security of Information Act 2001, s 15(4)(g).

any restriction to be necessary, responsive to a pressing social need and proportionate.[67]

7.136 If authorisation was declined, then the individual could seek judicial review of this decision.

7.137 By virtue of section 7(1) of the Official Secrets Act 1989, a disclosure made by a Crown servant, a member of the security and intelligence agencies or notified person is made with lawful authority if, and only if, it is made in accordance with an official duty. On its face, it seems as though there is no mechanism for current members of the security and intelligence agencies to seek authorisation to make a disclosure. Our preliminary consultation with stakeholders has confirmed, however, that a process for seeking authorisation to make a disclosure is included in the contract of employment of those who are members of the security and intelligence agencies. This process is intended to ensure Article 10 compliance.

7.138 Despite the fact that in practice there is already a process whereby authorisation to make a disclosure can be sought, we believe this is something that ought to be enshrined in legislation.

Provisional conclusion 27

7.139 **It should be enshrined in legislation that current Crown servants and current members of the security and intelligence agencies are able to seek authority to make a disclosure. Do consultees agree?**

7.140 Despite Lord Bingham's conclusion in *Shayler* that the authorisation process is compliant with Article 10 of the European Convention on Human Rights, we believe there are ways it could be improved. We believe that one way would be to enshrine in statute a non-exhaustive list of factors that ought to be taken into consideration when deciding whether authorisation to make a disclosure ought to be declined. This echoes the view that was taken in *Shayler*, in which Lord Bingham stated that authorisation should only be declined when disclosure of the information in question would be detrimental to national security and/or would cause damage to the work of the security and intelligence agencies.[68]

7.141 A non-exhaustive list would increase the predictability and transparency of the process and would act as an additional safeguard against decisions that do not have sufficient regard for the employee's right to freedom of expression, whilst also dealing with one of the criticisms Lord Hope made of the legislation in *Shayler*.[69]

Provisional conclusion 28

[67] *R v Shayler* [2002] UKHL 11; [2003] 1 AC 247, para 30.

[68] *R v Shayler* [2002] UKHL 11; [2003] 1 AC 247, para 30.

[69] *R v Shayler* [2002] UKHL 11; [2003] 1 AC 247, para 70-85. These are discussed in greater detail in Chapter 6.

7.142 **There should be a non-exhaustive list of the factors to be considered when deciding whether to grant lawful authority to make a disclosure. Do consultees agree?**

CHAPTER 8
LIST OF CONSULTATION QUESTIONS AND PROVISIONAL CONCLUSIONS

CHAPTER 2: THE OFFICIAL SECRETS ACTS 1911, 1920 AND 1939

Provisional conclusion 1

8.1 We provisionally conclude that the inclusion of the term "enemy" has the potential to inhibit the ability to prosecute those who commit espionage. Do consultees agree?

Provisional conclusion 2

8.2 Any redrafted offence ought to have the following features:

(1) Like the overwhelming majority of criminal offences, there should continue to be no restriction on who can commit the offence;

(2) The offence should be capable of being committed by someone who not only communicates information, but also by someone who obtains or gathers it. It should also continue to apply to those who approach, inspect, pass over or enter any prohibited place within the meaning of the Act.

(3) The offence should use the generic term "information" instead of the more specific terms currently relied upon in the Act.

8.3 Do consultees agree?

Consultation question 1

8.4 Should the term "safety or interests of the state", first used in the 1911 Act, remain in any new statute or be replaced with the term "national security"?

Consultation question 2

8.5 Do consultees have a view on whether an individual should only commit an offence if he or she knew or had reasonable grounds to believe that his or her conduct might prejudice the safety or interests of the state / national security?

Consultation question 3

8.6 Is the list of foreign entities contained in the Espionage Statutes Modernization Bill a helpful starting point in the domestic context? Do consultees have views on how it could be amended?

Provisional conclusion 3

8.7 We have provisionally concluded that an offence should only be committed if the defendant knew or had reasonable grounds to believe his or her conduct was capable of benefiting a foreign power. Do consultees agree?

Provisional conclusion 4

8.8 The list of prohibited places no longer accurately reflects the types of site that are in need of protection. Do consultees agree?

Consultation question 4

8.9 We consider that a modified version of the approach taken in the Serious Organised Crime and Police Act 2005 is a suitable alternative to the current regime. The Secretary of State would be able to designate a site as a "protected site" if it were in the interests of national security to do so. Do consultees agree?

Provisional conclusion 5

8.10 There are provisions contained in the Official Secrets Act 1911-1939 that are archaic and in need of reform. Do consultees agree?

Provisional conclusion 6

8.11 We consider that the references in the Official Secrets Acts 1911 and 1920 to sketches, plans, models, notes and secret official pass words and code words are anachronistic and in need of replacement with a sufficiently general term. Do consultees agree?

Provisional conclusion 7

8.12 The territorial ambit of the offences ought to be expanded so that the offences can be committed irrespective of whether the individual who is engaging in the prohibited conduct is a British Officer or subject, so long as there is a "sufficient link" with the United Kingdom. Do consultees agree?

Consultation question 5

8.13 Bearing in mind the difficulties inherent in proving the commission of espionage, do consultees have a view on whether the provisions contained in the Official Secrets Acts 1911 and 1920 intended to ease the prosecution's burden of proof are so difficult to reconcile with principle that they ought to be removed or do consultees take the view that they remain necessary?

Provisional conclusion 8

8.14 We provisionally conclude that the Official Secrets Acts 1911-1939 ought to be repealed and replaced with a single Espionage Act. Do consultees agree?

CHAPTER 3: THE OFFICIAL SECRETS ACT 1989

Provisional conclusion 9

8.15 We provisionally conclude that, as a matter of principle, it is undesirable for those who have disclosed information contrary to the Official Secrets Act 1989 to be able to avoid criminal liability due to the fact that proving the damage caused by the disclosure would risk causing further damage. Do consultees agree?

Provisional conclusion 10

8.16 We provisionally conclude that proof of the defendant's mental fault should be an explicit element of the offence contained in the Official Secrets Act 1989. Do consultees agree?

Consultation question 6

8.17 We welcome consultees' views on the suitability of shifting to non-result based offences to replace those offences in the Official Secrets Act 1989 that require proof or likelihood of damage.

Provisional conclusion 11

8.18 With respect to members of the security and intelligence agencies and notified persons, the offences should continue to be offences of strict liability. Do consultees agree?

Provisional conclusion 12

8.19 The process for making individuals subject to the Official Secrets Act 1989 is in need of reform to improve efficiency. Do consultees agree?

Consultation question 7

8.20 If consultees agree with provisional conclusion 12, do consultees have a view on whether these options would improve the efficiency of the process for making individuals subject to the Official Secrets Act 1989?

(1) Member of the security and intelligence services – As we have discussed, it is not entirely clear what is intended to be meant by the term "member". One option is to amend the term to clarify that employees, seconded and attached staff, in addition to those working under a contract of service, fall within the scope of the offence in section 1(1).

(2) Notified person – We have provisionally concluded that notification does serve a useful function and ought to be retained. We do believe, however, that there are two ways the process could be improved. First, new guidance could be issued clarifying when an individual ought to be subject to notification. Secondly, the length of time a notification is in force could be lengthened. It is possible, however, to envisage more fundamental reform that would further reduce the administrative burden. One option is to specify the types of post that ought to be subject to notification. Rather than focusing upon the individual, the focus would be on the post. A second option would be to replace the notification provisions and expand the scope of section 1(1) to anyone who has, or has had access to security and intelligence information by virtue of their office or employment or contract of services.

(3) Definition of Crown servant – We provisionally conclude that the process for expanding the definition of Crown servant ought to be streamlined and that it should be possible to make an officeholder a Crown servant for the purposes of the Official Secrets Act 1989 by way of primary legislation, in addition to the process set out in section 12 of the Act.

Provisional conclusion 13

8.21 We provisionally conclude that the maximum sentences currently available for the offences contained in the Official Secrets Act 1989 are not capable of reflecting the potential harm and culpability that may arise in a serious case. Do consultees agree?

Provisional conclusion 14

8.22 A disclosure made to a professional legal advisor who is a barrister, solicitor or legal executive with a current practising certificate for the purposes of receiving legal advice in respect of an offence contrary to the Official Secrets Act 1989 should be an exempt disclosure subject to compliance with any vetting and security requirements as might be specified. Do consultees agree?

Provisional conclusion 15

8.23 We provisionally conclude that a defence of prior publication should be available only if the defendant proves that the information in question was in fact already lawfully in the public domain and widely disseminated to the public. Do consultees agree?

Consultation question 8

8.24 We would welcome consultees' views on whether the categories of information encompassed by the Official Secrets Act 1989 ought to be more narrowly drawn and, if so, how.

Consultation question 9

8.25 Should sensitive information relating to the economy so far as it relates to national security be brought within the scope of the legislation or is such a formulation too narrow?

Provisional Conclusion 16

8.26 The territorial ambit of the offences contained in the Official Secrets Act 1989 should be reformed to enhance the protection afforded to sensitive information by approaching the offence in similar terms to section 11(2) of the European Communities Act 1972 so that the offence would apply irrespective of whether the unauthorised disclosure takes place within the United Kingdom and irrespective of whether the Crown servant, government contractor or notified person who disclosed the information was a British citizen. Do consultees agree?

Provisional conclusion 17

8.27 The Official Secrets Act 1989 ought to be repealed and replaced with new legislation. Do consultees agree?

CHAPTER 4: WIDER UNAUTHORISED DISCLOSURE OFFENCES

Consultation question 10

8.28 Do consultees agree that a full review of personal information disclosure offence is needed?

Consultation question 11

8.29 Do consultees have a view on whether the offence in section 55 of the Data Protection Act 1998 ought to be reviewed to assess the extent to which it provides adequate protection for personal information?

Consultation question 12

8.30 Do consultees have a view on whether national security disclosure offences should form part of a future full review of miscellaneous unauthorised disclosure offences?

CHAPTER 5: PROCEDURAL MATTERS RELATING TO INVESTIGATION AND TRIAL

Provisional conclusion 18

8.31 We provisionally conclude that improvements could be made to the Protocol. Do consultees agree?

Consultation question 13

8.32 Do consultees have a view on whether defining the term “serious offence” and ensuring earlier legal involvement would make the Protocol more effective?

Consultation question 14

8.33 Do consultees have views on how the Protocol could be improved?

Provisional conclusion 19

8.34 The power conferred on the court by section 8(4) of the Official Secrets Act 1920 ought to be made subject to a necessity test whereby members of the public can only be excluded if necessary to ensure national safety (the term used in the 1920 Act) is not prejudiced. Do consultees agree?

Provisional conclusion 20

8.35 The guidance on authorised jury checks ought to be amended to state that if an authorised jury check has been undertaken, then this must be brought to the attention of the defence representatives. Do consultees agree?

Provisional conclusion 21

8.36 A separate review ought to be undertaken to evaluate the extent to which the current mechanisms that are relied upon strike the correct balance between the right to a fair trial and the need to safeguard sensitive material in criminal proceedings. Do consultees agree?

CHAPTER 6: FREEDOM OF EXPRESSION

Provisional conclusion 22

8.37 Compliance with Article 10 of the European Convention on Human Rights does not mandate a statutory public interest defence. Do consultees agree?

CHAPTER 7: PUBLIC INTEREST DEFENCE

Provisional conclusion 23

8.38 The problems associated with the introduction of a statutory public interest defence outweigh the benefits. Do consultees agree?

Provisional conclusion 24

8.39 The legal safeguards that currently exist are sufficient to protect journalistic activity without the need for a statutory public interest defence. Do consultees agree?

Consultation question 15

8.40 We welcome views from consultees on the effectiveness of the Civil Service Commission as a mechanism for receiving unauthorised disclosures.

Provisional conclusion 25

8.41 A member of the security and intelligence agencies ought to be able to bring a concern that relates to their employment to the attention of the Investigatory Powers Commissioner, who would be able to investigate the matter and report their findings to the Prime Minister. Do consultees agree?

Provisional conclusion 26

8.42 The Canadian model brings no additional benefits beyond those that would follow from there being a statutory commissioner who could receive and investigate complaints from those working in the security and intelligence agencies. Do consultees agree?

Provisional conclusion 27

8.43 It should be enshrined in legislation that current Crown servants and current members of the security and intelligence agencies are able to seek authority to make a disclosure. Do consultees agree?

Provisional conclusion 28

8.44 There should be a non-exhaustive list of the factors to be considered when deciding whether to grant lawful authority to make a disclosure. Do consultees agree?

APPENDIX A
COMPARATIVE LEGAL ANALYSIS

A.1 This Appendix provides an overview of the law relating to the unauthorised disclosure of information in English speaking jurisdictions outside of the United Kingdom. In particular, the Appendix examines:

(1) Offences that criminalise:

(a) The unauthorised disclosure of information that is classified or relates to defence and national security.

(b) Espionage or working on behalf of a foreign government with intent to damage national security.

(2) Mechanisms that enable members of the security and intelligence agencies to make protected disclosures and raise concerns relating to their employment.

A.2 This Appendix examines the following jurisdictions:

(1) The United States of America.

(2) Canada.

(3) Australia.

(4) New Zealand.

(5) South Africa.

THE UNITED STATES OF AMERICA

A.3 This section will first outline the unauthorised disclosure and espionage offences that are applicable to all persons before outlining those unauthorised disclosure offences that are specific to government employees. The section will then outline the mechanisms available to make protected disclosures and briefly examine a number of issues arising under the current law.

A.4 The primary legislative provision that criminalises the unauthorised disclosure of specified categories of information is the Espionage Act 1917. This is supplemented by a collection of other statutes that protect information in certain specified circumstances. As noted by both the courts and legal scholars in the United States, the distinction between government employees and other persons is critical in the context of confidential information, particularly when it comes to constitutional protections. As such, the law is set out below to reflect these two categories of persons.

Unauthorised disclosure offences applicable to all persons

A.5 This section will examine the offences that criminalise unauthorised disclosures and espionage which are contained in the following statutes:

(1) The Espionage Act 1917.

(2) The Computer Fraud and Abuse Act 1989.

(3) The Economic Espionage Act 1996.

(4) Title 18 of the United States Code section 641.

(5) The Subversive Activities Control Act 1950.

(6) The Intelligence Identities Protection Act 1982.

The Espionage Act 1917 (18 United States Code sections 793 to 798) – Espionage activity

A.6 Sections 793(a) to (c) of the Espionage Act 1917 prohibit anyone from gathering, transmitting or obtaining (including attempts at transmitting or obtaining) national defence information. The fault element is intent for the information to be used to injure the United States or to advantage any foreign nation or reason to belief that the information will be used for either of these purposes. This section includes a long list of possible ways in which information may be gathered or transmitted.

A.7 Sections 793(d) and (e) are the central provisions of the Espionage Act 1917. It has been observed that they encompass a wide range of activities that bear little resemblance to "classic espionage".[1] They prohibit the disclosure, or attempted disclosure, of information relating to national defence to any person not entitled to receive such information. In addition, the subsections make it an offence to retain such information, or to fail to deliver it on demand to the officer or employee of the United States entitled to receive it. The fault element is wilfully disclosing,

[1] D Pozen, "The Leaky Leviathan: Why the Government Condemns and Condones Unlawful Disclosures of Information" (2013) 127 *Harvard Law Review* 512.

retaining or failing to deliver such information with reason to believe it could be used to injure the United States, or to the advantage of any foreign nation.

A.8 Although the subsections are drafted in such a way so as to distinguish between those who originally held the information lawfully (section 793(d)) and unlawfully (section 793(e)), the construction of the offences and the maximum punishment applicable to each are identical, namely a fine and/or 10 years' imprisonment.

A.9 In a recent case, the District Court of Virginia observed that, "section 793's litigation history is sparse… the modest number of reported decisions reflect that section 793 prosecutions are relatively rare".[2] The Supreme Court has considered and rejected a vagueness challenge to the phrase "information relating to the national defense", which is found in section 794. It has never reviewed sections 793(d) or (e).[3] At the circuit court level, authority also remains limited. There are two cases in which the lower courts have considered the constitutionality of section 793, which are considered below.

A.10 In *United States v Morison* the United States Court of Appeals for the Fourth Circuit interpreted the terms of section 793 in light of the due process clause of the Fifth Amendment to the United States Constitution. It was held that the term "information relating to national defence" requires the government to prove that the information is "closely held by the government"[4] and is of the type "that could be potentially damaging to the United States" if disclosed.[5] The court also made clear that whether the information "related to national defense" is a question of fact to be determined by the jury.[6]

A.11 It was held that the phrase "not entitled to receive" should be understood as incorporating the Executive Order establishing a uniform classification system for national security.[7] Furthermore, an intent requirement was read into the provisions in that the government must prove that the defendant knew the information was national defence information and that when he or she communicated the information he or she did so with "a bad purpose either to disobey or to disregard the law."[8]

A.12 It was argued in *Morison* that even if these provisions could be read as clear in their meaning, particularly with regards to whom they applied, they should be construed narrowly and strictly confined to conduct represented in "classic spying

2 *United States v Rosen* (2006) 445 F Supp 2d 602, by Judge Ellis.

3 *Gorin v. United States* (1941) 312 US 19.

4 *United States v Morison* (1988) 844 F 2d 1057, pp 1071-1072.

5 *United States v Morison* (1988) 844 F 2d 1057, p 1084. Though a more recent District Court decision, *United States v Kim*, Criminal No. 10-255 (CKK) (2013) declined to require the Government to disclose that the information would be potentially damaged to the United States or might be useful to an enemy of the United States. For further discussion see M Papandrea, "Leaker Traitor Whistleblower Spy: National Security Leaks and the First Amendment" (2014) 94 *Boston University Law Review* 449.

6 *United States v Morison* (1988) 844 F 2d 1057, pp 1073-1074.

7 *United States v Morison* (1988) 844 F 2d 1057, pp 1065-1066.

8 *United States v Morison* (1988) 844 F 2d 1057, p 1071.

and espionage activity".[9] The "classic case", the defendants argued, was the transmission of national defence information to agents of foreign governments, not the leaking of such information to the press.[10] This argument was rejected by the Court of Appeals for the Fourth Circuit on the grounds that the court could not replace the terms of a statute with what was characterised as being "unenacted legislative intent" when the provisions were in fact clear and conclusive.[11]

A.13 The court reaffirmed its earlier decision in *Boeckenhaupt v United States* that sections 793 and 794 were intended to criminalise separate and distinct wrongdoing.[12] In addressing the defendant's arguments, the Court of Appeals for the Fourth Circuit did note that in many cases, prosecutions under section 793 have tended to include counts under section 794.[13]

A.14 In the more recent case of *United States v Rosen*, the District Court of Virginia held that the term "information", which is found in sections 793(d) and (e) includes both tangible and intangible information. In this case, the defendant was accused of disclosing information relating to national defence. In the case of intangible information only, the requirement to prove intent, which was read into the provisions by the court in *Morison*, is coupled with an additional knowledge requirement. The court held that the purpose of this "is to heighten the government's burden when defendants are accused of communicating intangible information".[14] This additional fault element requires the prosecution to prove that such information was communicated with reason to believe it could be used to the injury of the United States or to the advantage of any foreign nation.

A.15 Section 794 encompasses what are considered the "traditional espionage" cases. Section 794(a) makes it an offence for anyone to disclose, or attempt to disclose, information, either directly or indirectly, that relates to national defence,[15] to any foreign government, any faction or party or military or naval force within a foreign country and any representative, officer, agent, employee, subject, or citizen of a foreign country. The fault element is that the disclosure was made with intent to injure the United States or to advantage a foreign nation or reason to believe that the information will be used to the injury of the United States or to the advantage of a foreign nation.

A.16 Section 794(b) applies "in time of war" and prohibits the communication of this information to the enemy or attempts to elicit any information relating to the public defence. The fault element is the same as for the offence in section 794(a). The offences contained in sections 794(a) and (b) are punishable by death or imprisonment for any term of years or for life.

[9] *United States v Morison* (1988) 844 F 2d 1057, p 1063.

[10] *United States v Morison* (1988) 844 F 2d 1057, p 1063.

[11] *United States v Morison* (1988) 844 F 2d 1057, p 1064.

[12] *United States v Morison* (1988) 844 F 2d 1057, p 1065.

[13] *United States v Morison* (1988) 844 F 2d 1057, p 1065.

[14] *United States v Rosen* (2006) 445 F Supp 2d 602, p 626.

[15] As discussed in relation to s 793, "information relating to the national defense" under section 794 has also been interpreted to mean that which is "closely held by the government". See *United States v Heine* (1945) 151 F 2d 813.

A.17 Section 798 makes it an offence for anyone to disclose certain classified information to an unauthorised person, or to publish or to use that information in any manner prejudicial to the safety or interests of the United States or for the benefit of any government to the detriment of the United States. The fault element is knowingly and wilfully disclosing, publishing or using that information. The punishment for violating this section is a fine or imprisonment of up to 10 years.

A.18 Sections 795 and 797 together prohibit the creation, publication, sale or transfer of photographs or sketches of vital military or naval defence installations or equipment, as designated by the President. The maximum sentence for committing the offence is a fine and/or one year's imprisonment.

The Computer Fraud and Abuse Act 1986 (18 United States Code section 1030) – Fraud and related activity in connection with computers

A.19 Section 1030(a)(1) punishes anyone who discloses, or attempts to disclose, classified information, retrieved by means of knowingly accessing a computer without, or in excess of, authorisation, to any person not entitled to receive the information, or wilfully retains the information and fails to deliver it on demand to the officer or employee of the United States entitled to receive it. The requisite fault element for this offence is reason to believe that such information could be used to injure the United States, or be to the advantage of any foreign nation. The punishment is a fine and/or imprisonment for up to 10 years.

The Economic Espionage Act 1996 (18 United States Code section 1831) – Economic espionage

A.20 This provision criminalises an individual who, intending or knowing that the offence will benefit any foreign government, foreign instrumentality, or foreign agent, knowingly—

(1) steals, or without authorisation appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains a trade secret;

(2) without authorisation copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys a trade secret;

(3) receives, buys, or possesses a trade secret, knowing the same to have been stolen or appropriated, obtained, or converted without authorisation;

(4) attempts to commit any offence described in any of paragraphs (1) through (3); or

(5) conspires with one or more other persons to commit any offence described in any of paragraphs (1) through (3), and one or more of such persons do any act to effect the object of the conspiracy.

A.21 The term "trade secret" means all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, programme devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether

tangible or intangible, and whether or how stored, compiled, or memorialised physically, electronically, graphically, photographically, or in writing if—

(1) the owner thereof has taken reasonable measures to keep such information secret; and

(2) the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, another person who can obtain economic value from the disclosure or use of the information;

A.22 The term "foreign instrumentality" means any agency, bureau, ministry, component, institution, association, or any legal, commercial, or business organization, corporation, firm, or entity that is substantially owned, controlled, sponsored, commanded, managed, or dominated by a foreign government.[16] The term "foreign agent" means any officer, employee, proxy, servant, delegate, or representative of a foreign government.[17]

A.23 The territorial ambit of the offence extends to conduct outside the United States if the offender is a natural person who is a citizen or permanent resident alien of the United States, or an organisation organised under the laws of the United States or a State or political subdivision thereof; or an act in furtherance of the offence was committed in the United States.[18]

A.24 The maximum sentence for an offence under this section is a fine not exceeding five million dollars and/or imprisonment for up to 15 years.[19]

18 United States Code section 641 – Theft of public money, property or records

A.25 This section punishes the theft or conversion of government property or records for one's own use or the use of another. This section does not explicitly prohibit the disclosure of classified information, but it has been used to prosecute individuals who leak information.[20] A person may be fined and/or imprisoned for up to ten years (if the property does not exceed the sum of $100). This provision also includes knowing receipt or retention of stolen property with the intent to convert it for the recipient's own use.

The Subversive Activities Control Act 1950 (50 United States Code Section 855) – Failure to register as an agent trained in foreign espionage systems

A.26 Sections 851 to 857 of Title 50 of the United States Code have their origins in the Foreign Agents Registration Act 1938. The Act was designed to limit the effect of

[16] 18 United States Code, s 1839(1).

[17] 18 United States Code, s 1839(2).

[18] 18 United States Code, s 1837.

[19] 18 United States Code, s 1831(a).

[20] J Elsea, *Criminal Prohibitions on the Publication of Classified Defense Information*, (Congressional Research Service, 9 September 2013) p 13.

foreign propaganda by revealing both the identity of foreign agents and the source of the propaganda they were disseminating.[21]

A.27 The Foreign Agents Registration Act 1938 was amended in 1950 by the Subversive Activities Control Act 1950, also known as the Internal Security Act, to require persons who had been trained in espionage, counter-espionage, or sabotage by foreign governments to register under the Foreign Agents Registration Act 1938.[22] This section, however, was repealed in 1956 and a new section was added expressly stating that persons who had knowledge or had received training in "espionage, counter espionage, or sabotage service or tactics of a government of a foreign country or of a foreign political party, shall register with the Attorney General".[23] This section was codified under 50 United States Code section 851.

A.28 Section 851 requires registration of persons who have knowledge of, or have received instruction or assignment in, espionage, counter-espionage or sabotage service or tactics of a foreign country or foreign political party. Section 851 provides:

> Every person who has knowledge of, or has received instruction or assignment in, the espionage, counter-espionage, or sabotage service or tactics of a government of a foreign country or of a foreign political party, shall register with the Attorney General by filing with the Attorney General a registration statement in duplicate, under oath, prepared and filed in such manner and form, and containing such statements, information, or documents pertinent to the purposes and objectives of this subchapter as the Attorney General, having due regard for the national security and the public interest, by regulations prescribes.

A.29 Rules and regulations promulgated pursuant to this Act are set forth in the Code of Federal Regulations.[24] Registration under the Foreign Agents Registration Act 1938 serves as the requisite notification.[25] The Code of Federal Regulations also sets out the material contents of the registration statement:

(1) The registrant's name, principal business address, and all other business addresses in the United States or elsewhere, and all residence addresses.

(2) The registrant's citizenship status and how such status was acquired.

[21] For a detailed background of the legislative history of the Foreign Agents Registration Act 1938, see M Spak, "America for Sale: When Well-Connected Former Federal Officials Peddle Their Influence to the Highest Foreign Bidder – A Statutory Analysis and Proposals for Reform of the Foreign Agents Registration Act and the Ethics in Government Act" (1989-1900) 78(2) *Kentucky Law Journal* 237 and CL Davis, "Attorneys, Propagandists, and International Business: A Comment on the FARA of 1938" (1973) 3 *Georgia Journal of International and Comparative Law* 408.

[22] Public Law No. 81-831, 64 Stat. 1005 (1950).

[23] Public Law No. 84-803, 70 Stat. 899 (1956).

[24] 28 Code of Federal Regulations, ss 12.1-12.70.

[25] 28 Code of Federal Regulations, s 12.3.

(3) A detailed statement setting forth the nature of the registrant's knowledge of the espionage, counterespionage, or sabotage service or tactics of a foreign government or foreign political party, and the manner in which, place where, and date when such knowledge was obtained.

(4) A detailed statement as to any instruction or training received by the registrant in the espionage, counterespionage, or sabotage service or tactics of a foreign government or foreign political party, including a description of the type of instruction or training received, a description of any courses taken, the dates when such courses commenced and when they ceased, and the name and official title of the instructor or instructors under whose supervision the courses were received as well as the name and location of schools and other institutions attended, the dates of such attendance, and the names of the directors of the schools and institutions attended.

(5) A detailed statement describing any assignment received in the espionage, counterespionage, or sabotage service or tactics of a foreign government or foreign political party, including the type of assignment, the date when each assignment began, the date of completion of each assignment, name and title of the person or persons under whose supervision the assignment was executed, and a complete description of the nature of the assignment and the execution thereof.

(6) A detailed statement of any relationship which may exist at the time of registration, other than through employment, between the registrant and any foreign government or foreign political party.

(7) Such other statements, information, or documents pertinent to the purposes and objectives of the act as the Attorney General, having due regard for the national security and the public interest, may require by this part or amendments thereto.[26]

A.30 Section 852 sets out the categories of person who are exempt from registration, they are any person:

(1) who has obtained knowledge of or received instruction or assignment in the espionage, counter-espionage, or sabotage service or tactics of a foreign government or foreign political party by reason of civilian, military, or police service or employment with the United States Government, the governments of the several States, their political subdivisions, the District of Columbia, the Territories, or the Canal Zone;

(2) who has obtained such knowledge solely by reason of academic or personal interest not under the supervision of or in preparation for service with the government of a foreign country or a foreign political party;

(3) who has made full disclosure of such knowledge, instruction, or assignment to officials within an agency of the United States Government having responsibilities in the field of intelligence, which disclosure has

[26] 28 Code of Federal Regulations, s 12.22.

been made a matter of record in the files of such agency, and concerning whom a written determination has been made by the Attorney General or the Director of Central Intelligence that registration would not be in the interest of national security;

(4) whose knowledge of, or receipt of instruction or assignment in, the espionage, counterespionage, or sabotage service or tactics of a government of a foreign country or of a foreign political party, is a matter of record in the files of an agency of the United States Government having responsibilities in the field of intelligence and concerning whom a written determination is made by the Attorney General or the Director of Central Intelligence, based on all information available, that registration would not be in the interest of national security;

(5) who is a duly accredited diplomatic or consular officer of a foreign government, who is so recognized by the Department of State, while he is engaged exclusively in activities which are recognized by the Department of State as being within the scope of the functions of such officer, and any member of his immediate family who resides with him;

(6) who is an official of a foreign government recognized by the United States, whose name and status and the character of whose duties as such official are of record in the Department of State, and while he is engaged exclusively in activities which are recognized by the Department of State as being within the scope of the functions of such official, and any member of his immediate family who resides with him;

(7) who is a member of the staff of or employed by a duly accredited diplomatic or consular officer of a foreign government who is so recognized by the Department of State, and whose name and status and the character of whose duties as such member or employee are a matter of record in the Department of State, while he is engaged exclusively in the performance of activities recognized by the Department of State as being within the scope of the functions of such member or employee;

(8) who is an officially acknowledged and sponsored representative of a foreign government and is in the United States on an official mission for the purpose of conferring or otherwise cooperating with United States intelligence or security personnel;

(9) who is a civilian or one of the military personnel of a foreign armed service coming to the United States pursuant to arrangements made under a mutual defense treaty or agreement, or who has been invited to the United States at the request of an agency of the United States Government; or

(10) who is a person designated by a foreign government to serve as its representative in or to an international organization in which the United States participates or is an officer or employee of such an organization or who is a member of the immediate family of, and resides with, such a representative, officer, or employee.

A.31 Section 855 creates an offence where a person:

> Wilfully violates any provision of this subchapter or any regulation thereunder, or in any registration statement wilfully makes a false statement of a material fact or wilfully omits any material fact, shall be fined not more than $10,000 or imprisoned for not more than five years, or both.

A.32 Section 856 makes failure to file a registration statement a continuing offence for as long as such failure exists, notwithstanding any statute of limitation or other statute to the contrary.

A.33 Despite the rigorous procedures laid down by the above sections, one commentator has called the system "inadequate" as:

> The only people who comply with the provisions of the Act are those who are not engaged in any surreptitious activity in the United States, or have effectively severed all connection with foreign espionage organizations.[27]

The Intelligence Identities Protection Act 1982 (50 United States Code sections 3121 to 3126) – Protection of certain national security information

A.34 Section 3121(a) encompasses those who have authorised access to classified information that identifies covert intelligence agents. Section 3121(b) encompasses those who come to learn the identity of covert agents through their authorised access to classified information. It is an offence intentionally to disclose any information that the discloser knows identifies a covert agent that the United States is taking measures to conceal to any individual not authorised to receive classified information. The offence is punishable by fine under title 18 or imprisonment for up to ten years, or both under section 121(a) and fifteen years under section 121(b).

A.35 Section 3121(c) also applies to those who come to learn of the identity of a covert agent in the course of a pattern of activities intended to identify and expose covert agents. There have been no cases interpreting the statute but there have been at least two convictions under the provision resulting from guilty pleas.[28]

Unauthorised disclosure offences specific to government employees

A.36 This part will outline the offences that criminalise unauthorised disclosure and espionage activity contained within the following statutes:

(1) Title 18 of the United States Code, section 1924.

(2) Title 18 of the United States Code, section 952.

(3) Title 50 of the United States Code, section 783.

(4) Title 18 of the United States Code, section 641.

[27] L Farago, *War of Wits: The Anatomy of Espionage and Intelligence* (1962).

[28] J Elsea, *Criminal Prohibitions on the Publication of Classified Defense Information*, (Congressional Research Service, 9 September 2013) p 14.

(5) The Uniform Code of Military Justice.

18 United States Code section 1924 – Unauthorised removal and retention of classified documents or material

A.37 Sections 1924(a) to (c) make it an offence for government employees, contractors and consultants who come into possession of classified material by virtue of their employment by the government to remove such material without authorisation. The section does not define who constitutes an officer, employee, contractor, or consultant of the United States. The fault element is knowingly removing material classified by the government as concerning national defence or foreign relations of the United States, with the intent to retain the materials at an unauthorised location. The offence is punishable by a fine of up to $1,000 and/or a prison sentence of up to one year.

18 United States Code Section 952 – Diplomatic codes and correspondence

A.38 This provision punishes individuals who, by virtue of their employment by the United States, wilfully publish or furnish to another, without authorisation, any official diplomatic code or material prepared in such a code. If found guilty, the offender may be punished by a fine and/or imprisonment for up to ten years. The wording of this provision suggests that former government employees who disclose material obtained during the course of their government employment would also fall within the scope of this offence.

50 United States Code Section 783 – Control of subversive activities

A.39 The Subversive Activities Control Act 1950, also known as the Internal Security Act, was codified under sections 781 to 858 of title 50 of the United States Code. Section 783(a) makes it an offence for any officer or employee of the United States, or any company that is owned "in major part" by the United States to communicate in any way to any person who the employee knows, or has reason to believe, to be an agent or representative of any foreign government, information which the discloser knows to be classified. Disclosure that has been specifically authorised by the President or the head of the department, agency or corporation does not come within the scope of this offence.

A.40 Section 783(b) also makes it an offence for any agent or representative of any foreign government knowingly to receive or attempt to receive, directly or indirectly, such classified information from such an officer or employee, unless, again, such disclosure has been authorised.

A.41 The punishment under section 783(c) is a fine of up to $10,000 and/or imprisonment for not more than ten years, in addition to being ineligible to hold any office, or place of honour, profit, or trust created by the Constitution or laws of the United States.

The Uniform Code of Military Justice (10 United States Code section 906a) - Espionage

A.42 The offence of espionage under Article 106a of the Uniform Code of Military Justice is codified in title 10 of the United States Code. Section 802 of the United States Code provides that members of the military suspected of espionage may be tried by court martial for violating Article 106a of the Uniform Code of Military

Justice. Espionage under Article 106a is defined in terms similar to those in 18 United States Code section 794. The maximum punishment is death if certain aggravating factors are present. Members of the military may also be tried by court martial for failure to obey an order or regulation (Article 92); aiding the enemy (Article 104); the general article which includes "all disorders and neglects to the prejudice of good order and discipline in the armed forces" (Article 134).

Analysis of unauthorised disclosure offences

A.43 Since the relevant legislation was enacted, there have been a number of prosecutions of those who have committed espionage. By comparison the number of prosecutions of government employees who have disclosed classified information to the press has been much lower.[29]

A.44 As of May 2014, seven government officials have been charged with offences relating to the unauthorised disclosure of classified information. Prior to 2009, there were only three instances in which a current or former government employee was charged with an offence for disclosing information to an unauthorised party.[30] Reasons for why prosecutions have been so rare were briefly discussed by the Court in *United States v Morison*:

> It is unquestionably true that the prosecutions generally under the Espionage Act, and not just those under section 793(d), have not been great. This is understandable. Violations under the Act are not easily established. The violators act with the intention of concealing their conduct. They try… to leave few trails. Moreover, any prosecution under the Act will in every case pose difficult problems of balancing the need for prosecution and the possible damage that a public trial will require by way of the disclosure of vital national interest secrets in a public trial.[31]

Constitutional challenges

A.45 The First Amendment to the US Constitution states: "Congress shall make no law… abridging the freedom of speech, or of the press". This guarantees individual's very broad, but not absolute, freedom to share information with others for the purposes of publication.[32] It is only in the most extreme situations, where disclosure of previously non-public information creates a clear and present danger of grave harm to the United States, that the individual might be punished for disclosing information.[33]

A.46 As mentioned earlier, in determining whether free speech rights enjoy this broad protection, the courts have emphasised the relationship to the government of the

[29] M Papandrea, "Leaker Traitor Whistleblower Spy: National Security Leaks and the First Amendment" (2014) 94 *Boston University Law Review* 449, p 531.

[30] S I Vladeck, "Prosecuting Leaks under U.S. Law" in *National Security, Leaks, Whistleblowers, and the Media: A Guide to the Law* (Paul Rosenzweig et al, ed 2014). For a list of US prosecutions of national security leakers see p 31.

[31] *United States v Morison* (1988) 844 F 2d 1057, p 1067.

[32] For a discussion see G Stone's statement to the Committee on the Judiciary, United States House of Representatives (16 December 2010).

[33] *Haig v Agee* (1981) 453 US 280.

person whose First Amendment rights are implicated. The District Court in *United States v Rosen* distinguished between two classes of people: those who access the information by virtue of their official position or employment and those who do not.[34]

Government employees and freedom of speech

A.47 A succinct summary of the protection government employees enjoy under the First Amendment, in light of the United States Supreme Court decision in *Snepp v United States,* is provided by Professor Geoffrey Stone:

> A public employee who discloses to a journalist or other disseminator classified information, the disclosure of which could appreciably harm the national security, has violated his position of trust, and ordinarily may be discharged and/or criminally punished without violating the First Amendment.[35]

A.48 In determining the scope of the protections offered to government employees who disclose information, it is instructive to look more generally at the Supreme Court's recent approach to government employees' free speech rights under the First Amendment.[36] In *Garcetti v Ceballos*, Justice Kennedy, writing for the majority, held that:[37]

> When public employees make statements pursuant to their official duties, the employees are not speaking as citizens for First Amendment purposes, and the Constitution does not insulate their communications from employer discipline.[38]

A.49 The court continued, however, to state that free speech could lawfully be restricted under the First Amendment were "that speech owes its existence to a public employee's professional responsibilities".[39] As the Court explained, this situation is to be contrasted with one where employees:

[34] *United States v Rosen* (2006) 445 F Supp 2d 602, p 635.

[35] G Stone's statement to the Committee on the Judiciary, United States House of Representatives (16 December 2010). For a critical discussion of Snepp v United States see M Papandrea, "Leaker Traitor Whistleblower Spy: National Security Leaks and the First Amendment" (2014) 94 Boston University Law Review 449, p 528.

[36] For a discussion of intelligence community insiders and the First Amendment see M Papandrea, "Leaker Traitor Whistleblower Spy: National Security Leaks and the First Amendment" (2014) 94 *Boston University Law Review* 449, pp 512-533.

[37] *Garcetti v Ceballos* (2006) 126 SC 1951. For a summary and discussion of the case see A Bernie, "Recent Developments: A Principled Limitation on Judicial Interference: *Garcetti v Ceballos*" (2007) 30(3) *Harvard Journal of Law and Public Policy* 1047, p 1058 and M Papandrea, "Leaker Traitor Whistleblower Spy: National Security Leaks and the First Amendment" (2014) 94 *Boston University Law Review* 449, pp 514-533.

[38] *Garcetti v Ceballos* (2006) 126 SC 1951, p 9, by Justice Kennedy.

[39] *Garcetti v Ceballos* (2006) 126 SC 1951, p 10, by Justice Kennedy.

> Are speaking as citizens about matters of public concern, they must face only those speech restrictions that are necessary for their employers to operate efficiently and effectively.[40]

A.50 Whilst *Garcetti v Ceballos* concerned an internal memo complaining about lower-level professional practices, the implications of the Court's principle of speaking "pursuant to official duties" and "owing to professional responsibilities" is in keeping with the outcome of *Snepp v United States*. Therefore, employee speech that consists of national security information obtained in the course of employment falls outside the protection of the First Amendment. It is important to note that in coming to this decision, the majority relied not only on concerns about judicial oversight of regulations between and among government employees, but also the existence of:

> The powerful network of legislative enactments – such as whistle-blower protection laws and labor codes – available to those who seek to expose wrongdoing.[41]

A.51 The issue arose again more recently in *Lane v Franks*.[42] The case required the Supreme Court to determine whether the First Amendment protects a public employee who provided truthful sworn testimony, compelled by subpoena, outside the course of his ordinary job responsibilities.

A.52 The Eleventh Circuit had held that because the respondent learned of the subject matter of his testimony in the course of his employment by the public body, *Garcetti v Ceballos* required that his testimony be treated as speech of an employee rather than a citizen. The Supreme Court disagreed with the approach taken by the lower court and held the respondent's sworn testimony to be the speech of a citizen, not an employee, and therefore protected by the First Amendment. Delivering the opinion of the unanimous court, Justice Sotomayor appeared to offer a narrower reading of the principle laid down by the court in *Garcetti v Ceballos*:

> *Garcetti* said nothing about speech that simply relates to public employment or concerns the information learned in the course of employment… In other words, the mere fact that a citizen's speech concerns information acquired by virtue of his public employment does not transform that speech into employee – rather than citizen – speech. The critical question is whether the speech at issue is itself ordinarily within the scope of an employee's duties, not whether it merely concerns those duties.[43]

A.53 As suggested by Vladeck in his analysis of the case, it could be argued that disclosing information without authorisation falls outside the scope of a government employee's duties. If so, employees may in fact enjoy the greater

[40] *Garcetti v Ceballos* (2006) 126 SC 1951, p 7, by Justice Kennedy. See also *Pickering v Board of Education* (1968) 391 US 563.

[41] *Garcetti v Ceballos* (2006) 126 SC 1951, p 14, by Justice Kennedy. See Justice Scouter's dissent p 13.

[42] *Lane v Franks* (2014) 573 US.

[43] *Lane v Franks* (2014) 573 US, p 10, by Justice Sotomayor.

protection offered to citizens than public employees under the First Amendment.[44] Indeed, in *Lane,* Justice Sotomayor noted the "special value" of speech by public employees on subject matters related to their employment– precisely because they gain knowledge of matters of public concern through their employment.[45]

A.54 It should be noted, however, that the free speech rights provided to citizens are not absolute; when they are speaking as citizens about matters of public concern, restrictions on employees are lawful where they are necessary for their employers to operate efficiently and effectively. In summary:

> It should be stressed that the scope of the First Amendment protections that might be available to a national security leaker today is hardly settled.[46]

The Espionage Act 1917 – Government employees

A.55 The constitutionality of section 793 of the Espionage Act 1917 arose in the case of *United States v Morison*. The defendant was employed at the Naval Intelligence Service Support Center and as part of his work had access to top secret information. In connection with his security clearance he had signed a non-disclosure agreement. The defendant released satellite photographs revealing construction of the first Soviet nuclear carrier to the editor of an annual English publication providing information on naval operations internationally. He claimed to have done so to alert the public to the scale of a Soviet naval build up.

A.56 The defendant was convicted of offences contrary to 18 United States Code Section 641 and section 793(d) and (e) of the Espionage Act 1917 on the basis that the statutes did not encompass the conduct he was charged with and, if they did, the provisions of the Espionage Act 1917 were unconstitutional.

A.57 In relation to the latter, the defendant argued that section 793(d) and section 793(e) were contrary to the protections guaranteed by the Fifth Amendment on the basis that they were insufficiently clear and precise. It was also argued that they infringed the defendant's freedom of expression to a degree greater than justified by the legitimate government need. Advancing this argument, the defendant pointed to the terms "relating to the national defence" and "wilfulness".

A.58 Hearing the appeal, the panel of the Court of Appeals for the Fourth Circuit held that no First Amendment rights were implicated in the defendant's case.[47] The court reiterated that the defendant was an employee of the intelligence service of

[44] S I Vladeck, "Prosecuting Leaks under U.S. Law" in *National Security, Leaks, Whistleblowers, and the Media: A Guide to the Law* (Paul Rosenzweig et al, ed 2014).

[45] *Lane v Franks* (2014) 573 US, p 10, by Justice Sotomayor.

[46] S I Vladeck, "Prosecuting Leaks under U.S. Law" in *National Security, Leaks, Whistleblowers, and the Media: A Guide to the Law* (Paul Rosenzweig et al, ed 2014).

the military establishment, who had been expressly notified of his obligations by the terms of his letter of agreement with the Navy. He committed the offence set out in section 793(d), and did so in a manner that sought to conceal his "secret" character of the information and his own identity as the person who disclosed it. Under these circumstances, the court held the First Amendment:

> Does not offer asylum…merely because the transmittal was to a representative of the press [or provide] a shield to immunize his act of thievery. To permit the thief thus to misuse the Amendment would be to prostitute the salutary purposes of the First Amendment.[48]

A.59 The court then proceeded to dismiss the arguments of vagueness and overbreadth under the Fifth Amendment.[49] Both terms were saved from constitutional challenge by the court's approval of the District Judge's more narrow definition of the terms in his instructions to the jury. The term "wilful" was interpreted as an act that:

> Is done voluntarily and intentionally and with the specific intent to do something that the law forbids. That is to say, with a bad purpose either to disobey or to disregard the law.[50]

A.60 The court held that the term "national defense" should be interpreted so as to include "all matters that directly or may reasonably be connected the defense of the United States against any of its enemies".[51] The Court of Appeals for the Fourth Circuit approved the District Judge's requirement that the government must prove that the disclosure, in this case of photographs, would be potentially damaging to the United States or might be useful to its enemies. In addition it was necessary to prove that the documents were closely held, meaning that they had not been made public and were not available to the general public.[52]

A.61 In summary, government employees may have their speech restricted in the circumstances set out in the provisions of the Espionage Act 1917, without violating the First Amendment.[53] This is because employees learn the information

[47] However, in their concurring judgments both Judge Wilkinson and Judge Phillips wrote separately to express their views that the First Amendment was implicated. For example, Justice Phillips wrote "I do not think the First Amendment interests here are insignificant. Criminal restraints on the disclosure of information threaten the ability of the press to scrutinize and report on government activity. There exists the tendency, even in a constitutional democracy, for government to withhold reports of disquieting developments and to manage news in a fashion most favourable to itself".

[48] *United States v Morison* (1988) 844 F 2d 1057, p 1068.

[49] While Morison's conviction was upheld by the Court, It is worth noting that on leaving office, President Clinton pardoned Morison.

[50] *United States v Morison* (1988) 844 F 2d 1057, p 1071.

[51] *United States v Morison* (1988) 844 F 2d 1057, p 1071.

[52] *United States v Morison* (1988) 844 F 2d 1057, p 1071.

[53] In *United States v Rosen* (2006) 445 F Supp 2d 602, p 635, Judge Ellis stated that the cases of *United States v Marchetti* (1972) 466 F 2d 1309 and *Snepp v United States* (1980) 444 US 507 stand for the more general proposition that government employees speech can be subjected to prior restraints where the government is seeking to protect its legitimate national security interests.

only by virtue of their government employment and had no right to know the information to begin with.[54] In their employment contracts, government employees will usually agree to abide by constitutionally permissible restrictions of their speech and are thus in a formal relationship of confidentiality with the government.

The Espionage Act 1917 – Non-Government employees

A.62 In so far as our research has been able to tell, there has never been a prosecution of a media organisation for publishing or disseminating unlawfully disclosed classified information.[55] Perhaps the closest case, and the one discussed in the context of the government restrictions on the free speech of non-government employees relating to national interest information, is *New York Times v United States*.[56] In this case the government attempted to place an injunction on the New York Times and Washington Post from publishing a copy of a top secret Defence Department study of the Vietnam War, known as the Pentagon Papers. The essence of the Supreme Court's response is captured in Justice Stewart's concurring opinion:

> We are asked… to prevent the publication… of material that the Executive Branch insists should not, in the national interest, be published. I am convinced that the Executive is correct with respect to some of the documents involved. But I cannot say that disclosure of any of them will surely result in direct, immediate, and irreparable damage to our nation or its people.[57]

A.63 In summary, the Supreme Court held that legislators and government officials have considerable power to keep classified information secret, but once that information gets released and into the hands of non-government individuals and organisations, there is much more limited power to restrict its further dissemination and publication.[58] That said, at least five of the Justices did suggest in their judgment that retrospective prosecutions for publishing unlawfully disclosed material relating to the national defence might be held to a less exacting First Amendment standard than had been applied in assessing the injunction or prior restriction.

A.64 The most recent authority on the constitutionality of the prosecution of non-government employees under the Espionage Act 1917 *United States v Rosen*, which was discussed above. It is the only example in the history of the Espionage

[54] *Seattle Times Co v Rhinehart* (1984) 467 US 20.

[55] G Stone's statement to the Committee on the Judiciary, United States House of Representatives (16 December 2010).

[56] *New York Times v United States* (1971) 403 US 713.

[57] *New York Times v United States* (1971) 403 US 713, p 730. Also cited in G Stone's statement to the Committee on the Judiciary, United States House of Representatives (16 December 2010).

[58] For a more detailed discussion of the impact of *New York Times v United States* (1971) 403 US 713 on possible prosecution of the publisher of information see J Elsea, *Criminal Prohibitions on the Publication of Classified Defense Information*, (Congressional Research Service, 9 September 2013), p 26. A majority of the Supreme Court Justices have suggested elsewhere that newspapers, as well as former government employees who leaked information to the press, could be prosecuted under the Espionage Act 1917.

Act 1917 of a prosecution being brought against someone other than the initial government official who disclosed the information.[59]

A.65 The case concerned two defendants who were employed by the American Israel Public Affairs Committee, a lobbying group that focuses on foreign policy issues of interest to Israel. The defendants obtained information from various government officials over a five-year period and transmitted this information to members of the media, officials of foreign governments and others within the American Israel Public Affairs Committee.[60]

A.66 They were prosecuted under sections 793(d) and (e) of the Espionage Act 1917. The defendants filed a pre-trial motion to dismiss the charges arguing that the provisions violated:

(1) the Fifth Amendment's due process clause on the basis that the provisions fail to define what kind of information falls within "information relating to the national defense" and which individuals are "not entitled to receive" that information; and

(2) the First Amendment, which offers extensive protection to freedom of expression. The defendants sought to distinguish the precedent set in *United States v Morison* and earlier cases by arguing the oral reception of the information in this case meant it was difficult to know at the time whether or not it was classified.

A.67 The United States District Court for the Eastern District of West Virginia denied the motion to dismiss. Judge Ellis confirmed that the principles earlier set out by the Court of Appeals for the Fourth Circuit in *United States v Morison* also apply to cases where information is retransmitted orally.

A.68 In relation to the second point, Judge Ellis accepted that the defendants' case was distinct from that of *United States v Morison*. The defendants here did not agree to restrain their speech as part of their employment, and accordingly, the protection afforded by the First Amendment was more robust. Invoking parts of the judgment from *New York Times v United States*, Judge Ellis concluded that:

> Both common sense and the relevant precedent point persuasively to the conclusion that the government can punish those outside of the government for the unauthorised receipt and deliberate retransmission of information relating to the national defense.[61]

A.69 Judge Ellis did emphasise, however, that:

[59] S I Vladeck, prepared statement before the Committee on the Judiciary House of Representatives, *Espionage Act and the Legal and Constitutional Issues Raised by Wikileaks*, 112th Congress, Second Session (16 December 2010).

[60] For a brief discussion of the facts surrounding the case see: http://www.nytimes.com/2009/05/02/us/politics/02aipac.html?_r=1 (last visited 22 November 2016).

[61] *United States v Rosen* (2006) 445 F Supp 2d 602, p 637.

> This conclusion rests on the limitation of section 793 to situations in which national security is genuinely at risk; without this limitation, Congress loses its justification for limiting free expression.[62]

A.70 Ultimately the prosecution in *United States v Rosen* was discontinued after the opinion of the court was delivered.[63] Nonetheless, the reasoning of Judge Ellis in *United States v Rosen* has been subject to criticism by Professor Harold Edgar. In particular, Edgar claims that the court "both misconstrued and overgeneralized" the judicial precedent on section 793(e) by relying on cases that did not in fact implicate First Amendment rights.[64]

A.71 Edgar further submits that the court should have applied the more rigorous test for vagueness that is required by the First Amendment to its reading of the terms of the Espionage Acts that were contested by the defendants. Had the court applied this approach, Edgar argues the Espionage Act 1917 would fail. In particular, Edgar points to the vagueness of "national defense', which he states makes it difficult for an ordinary person to determine its permissible scope, with a corresponding chilling effect on free speech, particularly in the media world, something which the Constitution exists specifically to prevent.[65]

Proposed reform of the Espionage Act 1917

A.72 Since 2000 there have been a number of attempts to reform the Espionage Act 1917. None of the proposed bills have been enacted.[66]

The Classified Information Protection Bill 2001

A.73 In 2000, 2001 and 2003, there were attempts to introduce provisions that would have made it an offence for an employee or former employee of the United States; or any other person with access to classified information knowingly or wilfully to disclose, or attempt to disclose, classified information to a person not authorised to access such information, knowing that this person is not authorised to access such information. What distinguishes these provisions from the current law is that they did not specify that an offence would only be committed if the information was to be delivered or intended to be used by foreign agents; or that damage to national security would result from the unauthorised disclosure.

A.74 President Clinton vetoed the bill in 2000, on the basis that it was overbroad and at risk of creating an unnecessary chill on legitimate activities in a democracy.[67]

[62] *United States v Rosen* (2006) 445 F Supp 2d 602, p 639.

[63] See http://www.nytimes.com/2009/05/02/us/politics/02aipac.html?_r=0 and T S Ellis, III, "National Security Trials: A Judge's Perspective" (2013) 99 *Virginia Law Review* 1607.

[64] H Edgar, "United States v Rosen" (2007) 120 *Harvard Law Review* 821, p 824.

[65] H Edgar, "United States v Rosen" (2007) 120 *Harvard Law Review* 821, p 824. Edgar cites in support the case of *Grayned v City of Rockford* (1972) 408 US 104, pp 108-109.

[66] J Elsea, *Criminal Prohibitions on the Publication of Classified Defense Information*, (Congressional Research Service, 9 September 2013), pp 27-30.

[67] Message on Returning Without Approval to the House of Representatives the "Intelligence Authorization Act for Fiscal Year 2001", 36 *Weekly Compilation of Presidential Documents* 278 (4 November 2000).

Securing Human Intelligence and Enforcing Lawful Dissemination Act 2010

A.75 The Securing Human Intelligence and Enforcing Lawful Dissemination Act would have amended the Espionage Act 1917 to make it a crime for any person knowingly or wilfully to disseminate in any manner, prejudicial to the safety or interest of the United States, any classified information concerning human intelligence activities in the United States.

A.76 The Bill was criticised for its application to individuals and organisations other than government employees. A number of scholars claimed this this would violate the First Amendment unless it was expressly limited to situations in which the dissemination at issue posed a clear and imminent danger of grave harm to the United States.[68]

The Espionage Statutes Modernization Act 2010

A.77 Section 355 of the Espionage Statutes Modernization Act 2010 sought to broaden the Espionage Act 1917 provisions by extending their coverage to:

(1) all classified information related to national security (rather than just national defence information);

(2) incorporating non-state threats into the prohibition by replacing "foreign government" or "foreign nation" with the term "foreign power"; and

(3) criminalising the intentional unauthorised disclosure of properly classified information by government employees, contractors or consultants in violation of their non-disclosure agreements.

A.78 The term "foreign power" was to be given the meaning contained in section 101 of the Foreign Intelligence Surveillance Act 1978, namely:

(1) a foreign government or any component thereof, whether or not recognized by the United States;

(2) a faction of a foreign nation or nations, not substantially composed of United States persons;

(3) an entity that is openly acknowledged by a foreign government or governments to be directed and controlled by such foreign government or governments;

(4) a group engaged in international terrorism or activities in preparation therefor;

(5) a foreign-based political organization, not substantially composed of United States persons;

(6) an entity that is directed and controlled by a foreign government or governments; or

[68] G Stone's statement to the Committee on the Judiciary, United States House of Representatives (16 December 2010), p 6.

(7) an entity not substantially composed of United States persons that is engaged in the international proliferation of weapons of mass destruction.[69]

The Criminal Code Modernization and Simplification Act 2011

A.79 If it had been enacted, Chapter 17, subchapter E of the Criminal Code would have remodeled the Espionage Act 1917 around three sections:

(1) a section prohibiting the gathering or transmission of defence material to any person not entitled to receive it, if done with the intent to injure the United States or advantage any foreign power or reason to believe it will injure the United States or advantage any foreign power;

(2) a section criminalising those in lawful possession or control of defence information that allow it to be recklessly lost, stolen or destroyed or fail to report such an incident to the appropriate officer; and

(3) a section prohibiting those who knowingly disclose classified or similarly protected information to a person not entitled to receive or use such information to injure the United States or advantage a foreign power.

Mechanisms that allow for the protected disclosure of official information

A.80 As discussed above, the First Amendment does not preclude government employees who disclose information related to national defence from being prosecuted under the Espionage Act 1917. There are, however, various mechanisms that enable categories of government employees to disclose classified national security information through official channels and designated persons and potentially to Congress.

A.81 This section will first outline the protection available for those who make unauthorised disclosures. In particular, this section will outline the mechanisms contained in the following provisions:

(1) The Whistleblower Protection Act 1989.

(2) The Intelligence Community Whistleblower Protection Act 1998.

(3) Presidential Policy Directive 19.

(4) The Military Whistleblower Protection Act 1988.

Whistleblower Protection Act 1989 (5 United States Code section 2302 and various other sections)

A.82 The Whistleblower Protection Act 1989 is codified in various parts of title 5 of the United States Code. The Whistleblower Protection Act 1989 provides protection for particular federal employees who make protected disclosures evidencing illegal or improper government activities through prescribed internal processes. It is important to note from the outset that the Whistleblower Protection Act 1989 affords protection specifically to federal employees who make protected

[69] 50 United States Code, s 1801(a).

disclosures as prescribed by section 2302(b)(8) of title 5 of the United States Code. Therefore, the Whistleblower Protection Act 1989 does not provide protection for unauthorised disclosures to the public at large or, as will be discussed, protection for the disclosure of information that is required by executive order to be kept secret in the interest of national defence.

A.83 In order to benefit from the protections of the Whistleblower Protection Act 1989, the following elements must be satisfied:

(1) an agency has taken, or failed to take, a "personnel action", which leads to a negative or adverse impact on the employee;

(2) the action was taken because of a "protected disclosure"; and

(3) the disclosure was made by a "covered employee".[70]

"PERSONNEL ACTION"

A.84 The Whistleblower Protection Act 1989 protects employees from a broad range of actions by the government which could have a negative or adverse impact on the employee. The statute specifically defines the term "personnel action" to include the following areas of agency activity:

(1) an appointment;

(2) a promotion;

(3) an action under chapter 75 or other disciplinary or corrective action;

(4) a detail, transfer, or reassignment;

(5) a reinstatement;

(6) a restoration;

(7) a reemployment;

(8) a performance evaluation under chapter 43 of this title;

(9) a decision concerning pay, benefits, or awards, or concerning education or training if the education or training may reasonably be expected to lead to an appointment, promotion, performance evaluation, or other action described in this subparagraph;

(10) a decision to order psychiatric testing or examination;

(11) the implementation or enforcement of any nondisclosure policy, form, or agreement; and

[70] For a helpful summary of the Whistleblower Protection Act 1989 see: J O Shimabukuro and L P Whittaker, "Whistleblower Protections Under Federal Law: An Overview" Congressional Research Service (13 September 2012), pp 15-22.

(12) any other significant change in duties, responsibilities, or working conditions.[71]

"PROTECTED DISCLOSURE"

A.85 Any disclosure of information by a covered employee will be protected provided that the employee reasonably believes that the information evidences:

(1) Any violation of any law, rule, or regulation.[72]

(2) Any gross mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety.[73]

A.86 The above applies, however, only if such disclosure:

> Is not specifically prohibited by law and if such information is not specifically required by Executive order to be kept secret in the interest of national defense or the conduct of foreign affairs.[74]

A.87 There are four forums where whistleblowers may lawfully make a protected disclosure. It should be noted that an aggrieved employee affected by a prohibited personnel action is precluded from relying upon more than one of the remedies below:

(1) An appeal by the employee to the Merit Systems Protection Board of an agency's adverse action against the employee under chapter 77. The Protection Board is authorised to hear and rule on some appeals by employees regarding agency actions affecting the employee.[75] An agency's decision and action will not be upheld if the employee "shows that the decision was based on any prohibited personnel practice described in section 2302(b) of this title".[76]

(2) Actions taken by the Office of Special Counsel. The Office was established by the Whistleblower Protection Act 1989 as an organisation independent from the board of the relevant organisation. It is tasked with receiving allegations of prohibited personnel practices and to investigate such allegations.[77] It can also conduct an investigation of possible prohibited personnel practices on its own initiative, without any allegation.[78] If the Special Counsel decides there are reasonable grounds to believe that a prohibited personnel practice has or will occur, the Special Counsel can communicate this to the agency head and require

[71] 5 United States Code, s 2302(a)(2)(A).

[72] 5 United States Code, s 2302(b)(8)(A)(i).

[73] 5 United States Code, s 2302(b)(8)(A)(ii).

[74] 5 United States Code, s 2302(b)(8)(A)(ii).

[75] 5 United States Code, ss 7701 and 1205.

[76] 5 United States Code, s 7701(c)(2)(B).

[77] 5 United States Code, s 1212(a)(2).

[78] 5 United States Code, s1214(a)(5).

him or her to conduct an investigation and submit a written report.[79] The identity of the complaining employee may not be disclosed without the individual's consent.[80] The Special Counsel then reviews the reports as to their completeness and the reasonableness of the findings[81] and submits the reports to Congress, the President, the Comptroller General[82] and the complainant.[83] If the agency does not act to correct the prohibited personnel practice, the Special Counsel may petition the board for corrective action.[84]

(3) The Whistleblower Protection Act 1989 provides that covered employees have the right to seek review of any whistleblower reprisal by the Protection Board. This must be sought no more than 60 days after notification is provided to such employee that the investigation was closed or 120 days after filing a complaint with the Special Counsel.[85]

(4) Beyond the statutory provisions of the Whistleblower Protection Act 1989, the defence or claim of reprisal for whistleblowing might also be raised in a grievance proceeding brought by the employee pursuant to a grievance procedure.

"COVERED EMPLOYEE"

A.88 A "covered employee" includes current and former employees, or applicants for employment to positions in the executive branch of government and the Government Printing Office, in both the competitive and the excepted service, as well as positions in the Senior Executive Service.[86] Significantly, though, it excludes employees who:

(1) Are excepted from the competitive service because of their "confidential, policy-determining, policy-making, or policy-advocating character".[87]

(2) Are excluded by the President based on a determination by the President that it is necessary and warranted by conditions of good administration.[88]

(3) Federal workers employed by the United States Postal Service or the Postal Rate Commission, the Government Accountability Office, the Federal Bureau of Investigation, the Central Intelligence Agency, the Defense Intelligence Agency, the National Geospatial-Intelligence

[79] 5 United States Code, s 1213(c)(1).

[80] 5 United States Code, s 1213(h). This section allows for an exception to anonymity where the Special Counsel determines that disclosure is necessary to avoid imminent danger to health and safety or an imminent criminal violence.

[81] 5 United States Code, s 1213(e)(2).

[82] 5 United States Code, s 1213(e)(3).

[83] 5 United States Code, s 1213(e)(1).

[84] 5 United States Code, s 1214(b)(2)(C).

[85] 5 United States Code, ss 1221 and 1214(a)(3).

[86] 5 United States Code, s 2302(a)(2)(B).

[87] 5 United States Code, s 2302(a)(2)(B)(i).

[88] 5 United States Code, s 2302(a)(2)(B)(ii).

> Agency, the National Security Agency, and any other executive entity that the President determines primarily conducts foreign intelligence or counter-intelligence activities.[89]

A.89 The result of these excepted classes of employees is that:

> For the vast majority of federal employees in possession of classified national security information, the [Whistleblower Protection Act 1989] is simply inapplicable.[90]

Intelligence Community Whistleblower Protection Act 1998 (5 United States Code section 1212 to 1214)

A.90 The Intelligence Community Whistleblower Protection Act 1998, codified in title 5 of the United States Code section 1212 to 1214, extends the protection granted by the Whistleblower Protection Act 1989 to members of the intelligence services who make protected disclosures.[91] The Intelligence Community Whistleblower Protection Act 1998 enables employees and contractors of the intelligence services to bring a complaint, or disclose specified information, to the agency head, and ultimately Congress. Whilst the Intelligence Community Whistleblower Protection Act 1998 outlines the procedures for making a protected disclosure, the Act does not expressly prohibit retaliation against members of the intelligence community for making a disclosure and contains no explicit mechanism for members to obtain a remedy for any such retaliation.

A.91 The Intelligence Community Whistleblower Protection Act 1998 applies to employees of the Central Intelligence Agency,[92] Defense Intelligence Agency, National Imagery and Mapping Agency, National Reconnaissance Office, National Security Agency, Federal Bureau of Investigation, and any other agency that the President determines has the principal function of conducting foreign intelligence or counterintelligence activities.[93] It also applies to the employees of a contractor of any of these agencies.[94]

A.92 Intelligence community employees and contractors can disclose complaints and information that are "with respect to an urgent concern" to the agency head through the agency channels described in the Intelligence Community Whistleblower Protection Act 1998, before bringing them to Congress.[95] An "urgent concern" is defined in the Act to mean one of three things:

89 5 United States Code, s 2302(a)(2)(B)(ii).

90 S I Vladeck, "The Espionage Act and National Security Whistleblowing After Garcetti" (2008) 57(5) *American University Law Review* 1531, p 1543.

91 For a helpful overview of the Intelligence Community Whistleblower Protection Act 1998 see R M Perry, **"**Intelligence Whistleblower Protections: In Brief", Congressional Research Service (2014).

92 50 United States Code, s 3517(d)(5).

93 5 United States Code appendix, s 8H.

94 50 United States Code, s 3517(d)(5)(A); 5 United States Code appendix, s 8H(a)(1)(A) and (B).

95 50 United States Code, s 3517(d)(5)(A); 5 United States Code appendix, s 8H(a)(1)(A) and (B).

(1) A serious or flagrant abuse, problem, violation of executive order or law, or deficiency in funding, agency administration, or agency operations involving classified information.[96]

(2) A false statement to, or wilful withholding from, Congress on an issue of material fact relating to intelligence activity funding, administration, or operation.[97]

(3) Adverse personnel action stemming from disclosure under the Intelligence Community Whistleblower Protection Act 1998.[98]

A.93 The Intelligence Community Whistleblower Protection Act 1998 requires that a complaint is made, or information is given, to the Inspector General of the Agency,[99] who then has 14 days to evaluate the credibility of the complaint or information.[100] If the Inspector General finds that the complaint or information is credible,[101] he or she must send a notice of this finding, along with the complaint or information, to the agency head within the 14 day period.[102]

A.94 The head of the relevant agency then has seven days from receipt of the Inspector General's notice to forward the notice, along with any of the agency head's comments, to the congressional intelligence committees.[103] The Intelligence Community Whistleblower Protection Act 1998 expressly states that action taken by the Inspector General and agency head pursuant to the Intelligence Community Whistleblower Protection Act 1998 is not subject to judicial review, unlike retaliation claims under the Whistleblower Protection Act 1989.[104]

A.95 The Intelligence Community Whistleblower Protection Act 1998 permits employees to contact the relevant intelligence committees directly if the Inspector General either does not find the complaint or information credible, or sends the agency head an inaccurate complaint or inaccurate information.[105] This, however, is subject to two limitations:

[96] 50 United States Code, s 3517(d)(5)(g)(i)(I); 5 United States Code appendix, s 8H(h)(1)(A).

[97] 50 United States Code, s 3517(d)(5)(g)(i)(II); 5 United States Code appendix, s 8H(h)(1)(B).

[98] 50 United States Code, s 3517(d)(5)(g)(i)(III); 5 United States Code appendix, s 8H(h)(1)(C).

[99] 50 United States Code, s 3517(d)(5)(A); 5 United States Code appendix, s 8H(a)(1)(A) and (B). Inspector Generals are generally intended to provide independent, objective audits and investigations of agency operations, among other things. For example, The Inspector General of the Intelligence Community is responsible for conducting independent investigations, inspections, and audits of programs and activities that the Director of National Intelligence is responsible for administering.

[100] 50 United States Code, s 3517(d)(5)(A); 5 United States Code appendix, s 8H(a)(1)(A) and (B).

[101] 50 United States Code, s 3517(d)(5)(B); 5 United States Code appendix, s 8H(b).

[102] 50 United States Code, s 3517(d)(5)(B); 5 United States Code appendix, s 8H(b).

[103] 50 United States Code, s 3517(d)(5)(C); 5 United States Code appendix, s 8H(c).

[104] 50 United States Code, s 3517(d)(5)(F); 5 United States Code appendix, s 8H(f).

[105] 50 United States Code, s 3517(d)(5)(D)(i); 5 United States Code appendix, s 8H(d)(1).

(1) before making such contact, the employee or contractor must give the agency head a statement of the complaint/information through the Inspector General, along with notice of intent to contact the intelligence committees directly;[106] and

(2) the employee or contractor must follow the agency head's direction, given through the Inspector General, on compliance with appropriate security practices when contacting the intelligence committees.[107]

Presidential Policy Directive 19

A.96 This Presidential Policy Directive offers members of the intelligence services falling within the scope of the Directive further protection against retaliation for protected disclosures.[108] The Directive is an attempt to address perceived shortcomings with the Intelligence Community Whistleblower Protection Act 1998, specifically the fact that the act does not provide explicit protection from retaliation for making a protected disclosure.[109]

A.97 The Policy Directive applies to employees of a "covered agency", which is defined as an executive department or independent establishment that contains an "intelligence community element". This includes the Central Intelligence Agency, National Security Agency, Defense Intelligence Agency, National Geospatial-Intelligence Agency, National Reconnaissance Office, and any other agency determined by the President as having foreign intelligence or counterintelligence activities as its principal function. It should be noted that the Directive explicitly excludes from its protection the Federal Bureau of Investigation. Intelligence community contractors are also absent from the directive.

A.98 Five forms of disclosure constitute "protected disclosures":

(1) Disclosures to the agency Inspector General, Director of National Intelligence or supervisors within the employee's direct chain-of-command. The employee must reasonably believe that the disclosure evidences:

(a) a violation of law; a rule; a regulation; or

(b) a gross mismanagement; a gross waste of funds; an abuse of authority; or a substantial and specific danger to public health or safety;

[106] 50 United States Code, s 3517(d)(5)(D)(ii)(I); 5 United States Code appendix, s 8H(d)(2)(A).

[107] 50 United States Code, s 3517(d)(5)(D)(ii)(II); 5 United States Code appendix, s 8H(d)(2)(B).

[108] For a helpful overview of the *Presidential Policy Directive 19* see R M Perry, **"**Intelligence Whistleblower Protections: In Brief", Congressional Research Service (2014).

[109] S Tily, "National Security Whistleblowing vs. Dodd Frank Whistleblowing" (2015) 80(3) *Brooklyn Law Review* 1191, p 1200.

(2) disclosures to congressional committees made pursuant to the Intelligence Community Whistleblower Protection Act 1998, discussed above;

(3) any disclosure of a violation of the Presidential Policy Directive;

(4) disclosures made pursuant to an investigation or proceeding involving a violation of Presidential Policy Directive 19;

(5) disclosures to Inspectors General. [110]

A.99 Intelligence agency employees who make protected disclosures as defined by the Presidential Policy Directive cannot, as a consequence, be subject to adverse personnel actions or have their access to classified information curtailed by an officer or employee of the agency.[111]

INTERNAL AGENCY REVIEW

A.100 The Policy Directive required intelligence agencies to certify, within 270 days of the Directive being issued, that they had internal procedures for reviewing allegations of wrongful personnel actions or impacts on access to classified information.[112] Having done so, the Directive requires that these agency procedures permit the relevant Inspectors General to review employee allegations of adverse personnel action or improper restriction of access to classified information and recommend agency heads take corrective action if a violation of the Directive has been found to have taken place.[113]

A.101 Such corrective action may include reinstatement, back pay, and legal fees.[114] Once an agency head receives an Inspector General's recommendation, the Directive requires that they "carefully consider" the recommendation and findings, and decide whether or not corrective action is appropriate.[115] The panel then has 180 days to determine whether improper retaliation occurred. If the panel concludes that such retaliation occurred, it can recommend that the agency head takes corrective action, and the agency head must "carefully consider" this recommendation.

EXTERNAL AGENCY REVIEW

A.102 After an employee has exhausted the internal agency review process, the Directive permits him or her to request external review to the three member Inspector General panel, chaired by the Inspector General of the Intelligence Community acting on behalf of the Director of National Intelligence.[116] Once such

[110] Presidential Policy Directive 19, F(5).

[111] Presidential Policy Directive 19, B.

[112] Presidential Policy Directive 19, A.

[113] Presidential Policy Directive 19, B.

[114] Presidential Policy Directive 19, B.

[115] Presidential Policy Directive 19, A.

[116] Presidential Policy Directive 19, C.

a request is made, the Inspector General can decide, within his or her discretion, to convene an external review panel.[117]

A.103 The Inspector General panel then has 180 days to determine whether improper retaliation occurred.[118] If the panel concludes that retaliation did occur, it can recommend that the agency head take corrective action, and the agency head must "carefully consider" this recommendation.[119] The agency head then has 90 days to inform the panel and the Director of National Intelligence of what, if any, action it takes.[120] Decisions of the Inspector General panel are not amenable to judicial review.[121]

Title VI of the Intelligence Authorization Act for Fiscal Year 2015 (50 United States Code 3234 and various other sections)

A.104 The Intelligence Authorization Act serves to codify in statute some of the protections contained in Presidential Policy Directive 19. It covers employees of the same agencies as listed in the Presidential Protection Directive 19, and again excludes the Federal Bureau of Investigation. The Intelligence Authorization Act makes the distinction between retaliation in the form of either personnel actions or in the form of adverse security clearance or information access that results from making protected disclosures.

PERSONNEL ACTIONS

A.105 The Act protects against disclosures made to the:

(1) Director of National Intelligence;

(2) Inspector General of the Intelligence Community;

(3) the head of the employing agency;

(4) the employing agency's Inspector General;

(5) Congressional intelligence committees; or

(6) A member of a congressional intelligence committee.[122]

A.106 The disclosure must be of information that the employee reasonably believes evidences a violation of federal laws or regulations, mismanagement, waste of funds, abuse of authority, or a substantial and specific danger to public health or safety.[123] Significantly, the Intelligence Authorization Act does not contain any mechanism to enforce its protection against retaliation by adverse personnel

[117] Presidential Policy Directive 19, C.

[118] Presidential Policy Directive 19, C.

[119] Presidential Policy Directive 19, C.

[120] Presidential Policy Directive 19, C.

[121] R M Perry, **"**Intelligence Whistleblower Protections: In Brief", Congressional Research Service (2014).

[122] 50 United States Code, s 3234(b).

[123] 50 United States Code, s 3234(b).

action. Rather it prohibits agency employees from taking adverse personnel action against other employees who make protected disclosures.[124] Enforcement is expressly left to the President.[125]

ADVERSE SECURITY CLEARANCE OR INFORMATION ACCESS

A.107 The disclosures that are protected when retaliation is in the form of adverse security clearance or information access are greater than those facing adverse personnel actions. In addition to the protected disclosures just outlined, those facing security clearance/information access also enjoy protection for disclosures:

(1) Disclosures made in accordance with the procedures outlined in the Intelligence Community Whistleblower Protection Act 1998.[126]

(2) Disclosures made while exercising a legal right of appeal or complaint, including testimony in connection with someone else exercising such a right, or cooperating with an Inspector General.[127] This is subject to the caveat that such disclosure does not result in the sharing of information that is classified under an executive order for national security reasons.[128]

A.108 The Intelligence Authorization Act's protections against adverse security or information access determinations also differ from its protections against adverse personnel actions. This is because it provides mechanisms for enforcing protection, rather than leaving enforcement to the discretion of the President. The Intelligence Authorization Act permits an employee 90 days from the adverse security clearance or information determination to use appeal procedures that the President was required to establish under this legislation.[129]

Military Whistleblower Protection Act 1988 (10 United States Code section 1034 and amended by the National Defense Authorization Act for Fiscal Year 2014 section 1714)

A.109 The Military Whistleblower Protection Act 1988 prohibits "unfavourable personnel action"[130] in the case of:

(1) Lawful communication to a member of Congress or an Inspector General.[131]

(2) Communication which the Armed Forces member reasonably believes evidences:

[124] 50 United States Code, s 3234(b).

[125] 50 United States Code, s 3234(c).

[126] 50 United States Code, s 3341(j)(1)(C).

[127] 50 United States Code, s 3341(j)(1)(D).

[128] 50 United States Code, s 3341(j)(1)(D).

[129] 50 United States Code, s 3341(j)(4)(A). The requirements and stages of the appeal procedure more generally are set out in detail in 50 United States Code, s 3341(j)(4).

[130] Defined in the Military Whistleblower Protection Act 1988, 10 United States Code, s 1034(2).

[131] Military Whistleblower Protection Act 1988, 10 United States Code, s 1034(a)(1).

(a) a violation of law or regulation;

(b) a gross mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety; or

(c) a threat by another member of the armed forces or employee of the Federal Government that indicates a determination or intent to kill or cause serious bodily injury to members of the armed forces or civilians or damage to military, Federal, or civilian property. Such communication, however, must be made to one of the official persons or organisations listed in section 1034 (b)(1)(B). The list includes a Member of Congress and the Inspector General, as well as a member of a Department of Defense or any person or organisation in the chain of command.[132]

A.110 Members of the armed forces have one year to bring forward allegations from the date on which the personnel action is alleged to have occurred.[133] If a member of the armed forces submits an allegation to an Inspector General of a personnel action that is prohibited by the Military Whistleblower Protection Act 1988, the Inspector General must "expeditiously determine" whether there is sufficient evidence to warrant an investigation of the allegation.[134]

A.111 If it is decided that there is insufficient evidence to warrant an investigation, the Inspector General must forward the matter to the Inspector General of the Department of Defense for review.[135] If it is then decided that there is sufficient evidence, the Inspector General is required to investigate expeditiously the allegation.[136] The results of the investigation must be determined by, or approved by, the Inspector General of the Department of Defense, regardless of whether the investigation itself is conducted by the Inspector General of the Department of Defense.[137]

A.112 The Inspector General conducting the investigation must submit a report on the results of the investigation to the Secretary of Defense and the Secretary of the military department concerned.[138] No later than 30 days after receiving a report, the relevant Secretaries must determine whether there is sufficient basis to conclude whether a personnel action prohibited by the Act has occurred.[139] If the relevant Secretary determines this to be the case, they shall:

[132] Military Whistleblower Protection Act 1988, 10 United States Code, s 1034(c)(2)(C).

[133] Military Whistleblower Protection Act 1988, 10 United States Code, s 1034(c)(5).

[134] Military Whistleblower Protection Act 1988, 10 United States Code, s 1034(c)(4)(A).

[135] Military Whistleblower Protection Act 1988, 10 United States Code, s 1034(c)(4)(C).

[136] Military Whistleblower Protection Act 1988, 10 United States Code, s 1034(c)(4)(D).

[137] Military Whistleblower Protection Act 1988, 10 United States Code, s 1034(c)(4)(E).

[138] Military Whistleblower Protection Act 1988, 10 United States Code, s 1034(e)(1).

[139] Military Whistleblower Protection Act 1988, 10 United States Code, s 1034(f)(1).

(1) order such action as is necessary to correct the record of a personnel action prohibited;[140] and

(2) take any appropriate disciplinary action against the individual who committed such prohibited personnel action.[141]

CANADA

A.113 This section will first outline the Security of Information Act 2001, which is the primary source of unauthorised disclosure and espionage offences in Canada. The section will then outline the mechanisms that allow for the protected disclosure of official information and briefly examine issues arising under the current legal framework.

The Security of Information Act 2001

A.114 The legal provisions in Canada that criminalise unauthorised disclosures have historically reflected those of the United Kingdom. The Official Secrets Act (Canada) 1939 replicated the provisions of the Official Secrets Acts 1911 and 1920 and, after various amendments, resulted in the enactment of the Official Secrets Act (Canada) 1981.[142]

A.115 Over half of the 22 Canadian prosecutions under the Official Secrets Act arose following the defection of a cipher clerk in the Soviet embassy in Ottawa in 1945, which revealed a series of Soviet spy rings operating in Canada. Only a handful of prosecutions have occurred since 1961.[143] The Official Secrets Act was the subject of sustained criticism over the decades.[144] The 1969 Royal Commission on security considered its provisions to be over-inclusive, writing that "the Canadian Official Secrets Act is an unwieldy statute, couched in very broad and ambiguous language".[145] Further concerns were expressed by the Canadian Law Reform Commission in 1986, which questioned whether the reverse onus test on the accused violated the Canadian Charter of Rights and Freedoms.[146]

[140] Military Whistleblower Protection Act 1988, 10 United States Code, s 1034(f)(2)(a).

[141] Military Whistleblower Protection Act 1988, 10 United States Code, s 1034(f)(2)(b).

[142] See for example S Cohen, "Freedom of Information and the Official Secrets Act" (1979) 25 *McGill Law Journal* 99, p 110: "the 1939 Act was scarcely a uniquely Canadian product. In essence, it was an amalgamation of the British Official Secrets Acts of 1911 and 1920".

[143] S A Cohen, *Official Secrets Act* (2 July 2006, *Historica Canada*) http://www.thecanadianencyclopedia.ca/en/article/official-secrets-act/ (last visited 22 November 2016).

[144] For example Mackenzie Commission, *Royal Commission on Security Report* (1969); S Cohen, "Freedom of Information and the Official Secrets Act" (1979) 25(1) *McGill Law School* 99; M Rankin, "National Security: Information, Accountability, and the Canadian Security Intelligence Service" (1986) 36(3) *University of Toronto Law Journal* 249.

[145] Mackenzie Commission, *Reports of the Royal Commission on Security* (1969), p 75.

[146] Law Reform Commission of Canada, *Crimes Against the State* (1986) Working Paper 49.

A.116 In 2001, in the aftermath of the terrorist attacks in the United States of America,[147] the Official Secrets Act 1981 was substantially amended and renamed the Security of Information Act 2001.[148]

A.117 To date, there have been only two prosecutions under the Security of Information Act 2001**,** both of which involved defendants disclosing protected information to another state. The first of these prosecutions concerned Jeffrey Paul Delisle, who sold secret information that he had access to as a naval intelligence officer to the Russian military intelligence service between 2007 and 2012. He pleaded guilty in 2012 to two charges under the Act for having transmitted, and having attempted to transmit, protected information to a foreign entity, as well as a charge of breach of trust under the Canadian Criminal Code**.** In 2013 he was sentenced to 20 years' imprisonment and fined $111,817, an amount equal to what the Russians had paid him for the disclosure of the information.[149]

A.118 The second person to be prosecuted is Qing Quentin Huang, for communicating and attempting to communicate to a foreign entity information that the Government of Canada was taking measures to safeguard, and for breach of trust under the Criminal Code. A trial date for Quentin Huang has not yet been set.[150]

A.119 It should be noted that no prosecution for an offence under the Security of Information Act 2001 can be commenced without the consent of the Attorney General.[151]

Section 4 – Wrongful use of protected information

A.120 Section 4 of the Security of Information Act 2001 criminalises the wrongful use of protected information. This provision applies to anyone who has in their possession or control any secret official code word, password, sketch, plan, model, article, note, document or information that:

(1) relates to, or is used in, a prohibited place or that has been made or obtained in contravention of the Security of Information Act 2001; or has been obtained or had access to while subject to the Code of Service Discipline; or

(2) the person possesses due to their position as a person who holds or has held office under Her Majesty; a person who holds or is held to a contract made on behalf of Her Majesty or a contract carried out in a prohibited

[147] J McMenemy, *The Language of Canadian Politics: A Guide to Important Terms and Concepts* (4th ed 2006).

[148] RSC 1985, c 0-5, renamed the *Security of Information Act* by SC 2001, c 41, ss 24 and 25. See C Forcese "Clouding Accountability: Canada's Government Secrecy and National Secuirty Law "Complex"" (2005) 36 *Ottawa Law Review* 49 and K Roach "Ten Ways to Improve Canadian Anti-Terrorism Law" (2005-2006) 51 *Criminal Law Quarterly* 102.

[149] Public Prosecution Service of Canada, *Annual Report 2012-2013* (2013) <http://www.ppsc-sppc.gc.ca/eng/pub/ar-ra/2012_2013/index.html> (last visited 22 November 2016).

[150] Public Prosecution Service of Canada, *Annual Report 2014-2015* (2015) <http://www.ppsc-sppc.gc.ca/eng/pub/ar-ra/2014_2015/index.html> (last visited 22 November 2016).

[151] Security of Information Act 2001, s 24.

place; a person who is employed under person who holds or has held such an office or contract.[152]

A.121 The phrase "prohibited place" is defined in section 2(1) to mean:

(1) any work of defence belonging to or occupied or used by or on behalf of Her Majesty, including arsenals, armed forces establishments or stations, factories, dockyards, mines, minefields, camps, ships, aircraft, telegraph, telephone, wireless or signal stations or offices, and places used for the purpose of building, repairing, making or storing any munitions of war or any sketches, plans, models or documents relating thereto, or for the purpose of getting any metals, oil or minerals of use in time of war;

(2) any place not belonging to Her Majesty where any munitions of war or any sketches, plans, models or documents relating thereto are being made, repaired, obtained or stored under contract with, or with any person on behalf of, Her Majesty or otherwise on behalf of Her Majesty; and

(3) any place that is for the time being declared by order of the Governor in Council to be a prohibited place on the ground that information with respect thereto or damage thereto would be useful to a foreign power.

A.122 Section 4(1) provides that it is an offence for a person to:

(1) Communicate this information to anyone besides the person they are authorised to communicate it to, unless it is a person to whom it is in the interests of the state to communicate it to.[153]

(2) Use the information for the benefit of any foreign power or any other manner prejudicial to the safety or interests of the state.[154]

(3) Retain the information in their possession or control when they have no right to do so or fail to return or dispose of the information when lawfully requested.[155]

(4) Fail to take reasonable care of, or endanger the safety, of the information.[156]

A.123 Section 3(1) sets out an exhaustive list of acts that are regarded as being "prejudicial to the safety or interests of the state". The provision states that a purpose is prejudicial to the safety or interests of the State if a person:

(1) commits, in Canada, an offence against the laws of Canada or a province that is punishable by a maximum term of imprisonment of two years or

[152] Security of Information Act 2001, s 4(1).

[153] Security of Information Act 2001, s 4(1)(a).

[154] Security of Information Act 2001, s 4(1)(b).

[155] Security of Information Act 2001, s 4(1)(c).

[156] Security of Information Act 2001, s 4(1)(d).

more in order to advance a political, religious or ideological purpose, objective or cause or to benefit a foreign entity or terrorist group;

(2) commits, inside or outside Canada, a terrorist activity;

(3) causes or aggravates an urgent and critical situation in Canada that

(a) endangers the lives, health or safety of Canadians, or

(b) threatens the ability of the Government of Canada to preserve the sovereignty, security or territorial integrity of Canada;

(4) interferes with a service, facility, system or computer program, whether public or private, or its operation, in a manner that has significant adverse impact on the health, safety, security or economic or financial well-being of the people of Canada or the functioning of any government in Canada;

(5) endangers, outside Canada, any person by reason of that person's relationship with Canada or a province or the fact that the person is doing business with or on behalf of the Government of Canada or of a province;

(6) damages property outside Canada because a person or entity with an interest in the property or occupying the property has a relationship with Canada or a province or is doing business with or on behalf of the Government of Canada or of a province;

(7) impairs or threatens the military capability of the Canadian Forces, or any part of the Canadian Forces;

(8) interferes with the design, development or production of any weapon or defence equipment of, or intended for, the Canadian Forces, including any hardware, software or system that is part of or associated with any such weapon or defence equipment;

(9) impairs or threatens the capabilities of the Government of Canada in relation to security and intelligence;

(10) adversely affects the stability of the Canadian economy, the financial system or any financial market in Canada without reasonable economic or financial justification;

(11) impairs or threatens the capability of a government in Canada, or of the Bank of Canada, to protect against, or respond to, economic or financial threats or instability;

(12) impairs or threatens the capability of the Government of Canada to conduct diplomatic or consular relations, or conduct and manage international negotiations;

(13) contrary to a treaty to which Canada is a party, develops or uses anything that is intended or has the capability to cause death or serious bodily injury to a significant number of people by means of

(a) toxic or poisonous chemicals or their precursors,

(b) a microbial or other biological agent, or a toxin, including a disease organism,

(c) radiation or radioactivity, or

(d) an explosion; or

(14) does or omits to do anything that is directed towards or in preparation of the undertaking of an activity mentioned in any of paragraphs (1) to (14).

A.124 In one of the few cases interpreting the earlier Official Secrets Act 1981, the District Court of Montreal held that the words "secret official" qualify not only "code word or password" but also the rest of the clause, which means that the term "information" should be read as "secret and official information".[157] Although this case concerned the use of the term "secret official" under section 3(1)(c) of the Official Secrets Act 1939, it may still be instructive when interpreting the Security of Information Act 2001.

A.125 Section 4(3) makes it an offence for a person to receive any secret official item or information if they know, or have reasonable grounds to be believe at the time of receiving it, that such information is communicated to them in contravention of the Security of Information Act 2001. No offence takes place if the person can prove that the communication of the information was contrary to their desire.

A.126 Section 4(4) concerns official documents, even if they do not contain secret information. The provision makes it an offence to:

(1) retain any official document for any purposes which are prejudicial to the safety or interests of the State when the individual has no right to retain it or fails to comply with a lawful request to return or dispose of it (thereby introducing the "safety or interests of the State" criteria absent in section 4(1));

(2) allow any other person to have possession of any official document issued for their use alone;

(3) communicate any secret official code word or password;

(4) have in possession any official document or secret official code word or password issued to someone else (without lawful authority or excuse); or

(5) obtain an official document and neglect or fail to restore it to the person to whom it was issued or to the police (creating a positive duty to return the information even if not requested to do so).

Sections 13 and 14 – Those permanently bound to secrecy

A.127 For those permanently bound to secrecy, it is an offence for a person to, without lawful authority, communicate or confirm information that, if it were true, would

[157] Judgement No 5626, Court of Preliminary Inquiry, District of Montreal (unreported). See K Aquilina, "A study of section 3 of the Maltese Official Secrets Act, its Canadian and British counterparts and its effects on freedom of expression" (2013) 39(3) *Commonwealth Law Bulletin* 553.

amount to "special operational information".[158] It is irrelevant whether the information was true or not.[159] The fault element is the intention to communicate or confirm information that, if it were true, would be special operational information.

A.128 The phrase "permanently bound to secrecy" is defined in section 8(1) to mean:

(1) a current or former member or employee of a department, division, branch or office of the federal public administration or any of its parts;

(2) a person who has been served with a notice that they are permanently bound to secrecy under the power vested in a deputy head of a department under section 10(1) of the Security of Information Act 2001.

A.129 The phrase "special operational information" is defined in section 8(1) to mean information that the Canadian government is taking measures to safeguard that reveals, or from which may be inferred, anything listed in section 8(1)(a) to (g). This includes:

(1) covert human intelligence sources;

(2) the subject or objects of covert intelligence operations; and

(3) the nature or content of plans of the Canadian government for military operations in respect of a potential, imminent or present armed conflict.

A.130 It should be noted that this section does not specifically mention national security or national defence and most provisions relate to protecting covert intelligence sources and operations. The offence is punishable by imprisonment for up to five years less a day.[160]

A.131 Section 14(1) replicates this offence with regards to information that is *in fact* special operational information. Therefore, section 13 provides for instances where the information is purported to be, or not in fact, special operational information. The offence under section 14(1) is punishable by up to 14 years' imprisonment.[161]

Section 15 - Public interest defence for offences in section 13 and 14

A.132 There is a public interest defence for those bound to secrecy who disclose special operational information provided a number of criteria are met:

(1) First, the court must determine[162] that the person acted for the purpose of disclosing a statutory offence that they reasonably believed to have been, was being, or was about to be, committed by someone in the

[158] Security of Information Act 2001, s 13(1).

[159] Security of Information Act 2001, s 13(2).

[160] Security of Information Act 2001, s 13(3).

[161] Security of Information Act 2001, s 14(2).

[162] Security of Information Act 2001, s 15(3).

purported performance of that person's duties and functions for the Canadian government.[163]

(2) Secondly, the court must then decide whether the person has complied with prior disclosure regulations set out in sections 15(5)(a) to (b) of the Security of Information Act 2001. This section sets out the persons to whom the concern and relevant information must first be brought. First, the person must have brought the concern to his or her deputy head or, if not reasonably practical in the circumstances, the Deputy Attorney General of Canada. Second, where the person has not received a response from the above persons, the person must have brought his or her concern to the Security Intelligence Review Committee or the Communications Security Establishment Committee.[164] An exception to the disclosure requirements set out in section 15(5) is provided in circumstances where the communication or confirmation of the information was necessary to avoid grievous bodily harm or death.[165]

(3) Thirdly, if both of these conditions are met, the court may then move to consider whether the public interest in disclosure outweighs the public interest in non-disclosure. In deciding where the balance lies, the court must consider the following factors:

(a) whether the extent of the disclosure is no more than is necessary to disclose the alleged offence/prevent its commission;

(b) the seriousness of the alleged offence;

(c) whether the person resorted to other reasonably accessible alternatives and in doing so complied with any relevant guidelines, policies, or laws applicable;

(d) whether the person had any reasonable grounds to believe that the disclosure would be in the public interest;

(e) the public interest intended to be served by the disclosure;

(f) the extent of the harm/risk of harm created by the disclosure; and

(g) the existence of exigent circumstances justifying the disclosure.[166]

Section 4(2) – Communicating munitions of war information

A.133 Similar to section 4(1), section 4(2) makes it an offence to communicate information relating to munitions of war, directly or indirectly, to any foreign power or in any other manner prejudicial to the safety or interests of the state. This

[163] Security of Information Act 2001, s 15(2)(a).

[164] Security of Information Act 2001, s 15(5)(a).

[165] Security of Information Act 2001, s 15(6).

[166] Security of Information Act 2001, s 15(4)(a) to (g).

section may be considered closer to the "traditional espionage" than the previous two offences.

A.134 The phrase "munitions of war" is defined by section 2(1) to mean arms, ammunition, implements or munitions of war, military stores or any articles deemed capable of being converted into these things or useful in their production.

A.135 The phrase "foreign power" is defined by section 2(1) to mean:

(1) the government of a foreign state;

(2) an entity exercising or purporting to exercise the functions of a government in relation to a territory outside of Canada (regardless of whether Canada recognises the territory as a state); or

(3) a political faction or party operating within a foreign states whose purported purpose is to assume the role of government.

Section 16 – Communicating safeguarded information

A.136 Section 16(1) makes it an offence to communicate to a foreign entity or terrorist group information that the Canadian government (federal or provincial) is taking measures to safeguard. There are two fault element requirements:

(1) the person must believe, or be reckless to whether, it is information the Canadian government is taking measures to safeguard; and

(2) the person must intend by communicating the information to increase the capacity of a foreign entity or a terrorist group to harm Canadian interests, or be reckless as to the likelihood of this occurring.

A.137 Section 16(2) is similar to the offence in section 16(1), but extends it to cases where a person intentionally and without lawful authority communicates such information to a foreign entity or to a terrorist group and this actually results in harm to Canadian interests.

A.138 The phrase "foreign entity" is defined by section 2(1) to mean either:

(1) a foreign power;

(2) a group or association of foreign powers, or of one or more foreign powers and one or more terrorist groups; or

(3) a person acting at the direction of, for the benefit of, or in association either of those just listed.

A.139 The phrase "harm to Canadian interests" is defined by section 3(2) to mean a foreign entity or terrorist group that does anything referred to in paragraphs s.3(1)(a) to (n), which is the list for "prejudicial to the safety or interests of the state" discussed earlier.

A.140 A person who commits an offence under either of these provisions is liable to a maximum sentence of imprisonment for life.[167]

Section 17 – Communicating special operational information

Section 17(1) makes it an offence to communicate special operational information to a foreign entity or a terrorist group without lawful authority. Again, there are two fault element requirements: first, an intention to communicate such information and second, a belief, or recklessness as to whether, the information is special operational information. The sentence for this offence is imprisonment for life.[168]

Section 18 – Taking measures to safeguard information

A.141 Every person with government security clearance commits an offence if they communicate, or agree to communicate, to a foreign entity or to a terrorist group any information that is of a type the Canadian government is taking measures to safeguard, without lawful authority to do so. The fault element is having the intention to communicate.[169] A person found guilty under this offence is liable to up two years' imprisonment.[170]

Section 19 - Trade secrets and foreign economic entities

A.142 Section 19(1) makes it an offence to: communicate a trade secret to another person group or organisation[171] or obtain, retain, alter or destroy a trade secret.[172] In order to fall within this provision, a person must commit this prescribed conduct at the direction of, for the benefit of, or in association with a foreign economic entity, fraudulently and to the detriment of Canada's economic interest, international relations or national defence or national security. Whilst this is a form of economic espionage, the Security of Information Act 2001 nonetheless extends the offence to cover the impact this might have on national defence and security.

A.143 The phrase "foreign economic entity" is defined by section 2(1) to mean either:

(1) a foreign state or a group of foreign states; or

(2) an entity that is controlled, in law or in fact, or is substantially owned, by a foreign state or a group of foreign states.

A.144 The phrase "trade secret" is defined in section 19(4) to mean any information, including a formula, pattern, compilation, program, method, technique, process, negotiation position or strategy or any information contained or embodied in a product, device or mechanism that:

[167] Security of Information Act 2001, s 16(3).

[168] Security of Information Act 2001, s 17(2).

[169] Security of Information Act 2001, s 18(1).

[170] Security of Information Act 2001, s 18(2).

[171] Security of Information Act 2001, s 19(1)(a).

[172] Security of Information Act 2001, s 19(1)(b).

(1) is or may be used in trade or business;[173]

(2) is not generally known in that trade or business;[174]

(3) has economic value from not being generally known;[175] or

(4) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.[176]

A.145 Section 19(3) provides a statutory defence whereby a person is not guilty if the trade secret was either obtained by independent development or by reason only of reverse engineering,[177] or, acquired in the course of the person's work and is of such a character that its acquisition amounts to no more than an enhancement of that person's personal knowledge, skill or expertise.[178] The maximum sentence for committing the offence is 10 years' imprisonment.[179]

Sections 22 and 23 – Inchoate offences

A.146 Section 22 makes it an offence to do anything that is specifically directed towards, or done in preparation of, the commission of an offence under section 16(1), 17(1) or 19(1). Section 22 lists the acts which may be included in the terms "directed towards or specifically done in preparation of the commission of the offence". This includes simply "obtaining, retaining or gaining access to any information".[180]

A.147 Section 23 creates a separate offence for conspiring or attempting to commit an offence under the Security of Information Act 2001, or being an accessory after the fact in relation to an offence. Such a person will be liable to the same punishment and is to be proceeded against in the same manner as if they had committed the offence under the Security of Information Act 2001.

Mechanisms that allow for the protected disclosure of official information

A.148 This section will outline the protection available for those who make protected disclosures. In particular, this section will outline the following avenues of protection:

(1) The Public Servants Disclosure Protection Act 2007.

(2) Section 425.1 of the Canadian Criminal Code.

[173] Security of Information Act 2001, s 19(4)(a).

[174] Security of Information Act 2001, s 19(4)(b).

[175] Security of Information Act 2001, s 19(4)(c).

[176] Security of Information Act 2001, s 19(4)(d).

[177] Security of Information Act 2001, s 19(3)(a).

[178] Security of Information Act 2001, s 19(3)(a).

[179] Security of Information Act 2001, s 19(2).

[180] Security of Information Act 2001, s 22(1)(b).

Public Servants Disclosure Protection Act 2007

A.149 This is Canada's federal legislation for public sector employees to make protected disclosures.[181] The preamble of the Act captures the tension that its provisions are trying to ameliorate:

> Public servants owe a duty of loyalty to their employer and enjoy the right to freedom of expression as guaranteed by the Canadian Charter of Rights and Freedoms and that this Act strives to achieve an appropriate balance between those two important principles.

A.150 The Public Servants Disclosure Protection Act 2007 establishes the Public Sector Integrity Commissioner, the Public Servants Disclosure Protection Tribunal,[182] a requirement for the Treasury Board to establish a code of conduct applicable to the public sector,[183] as well as for the chief executives of public sector departments to establish their own codes of conduct for their respective departments.[184]

A.151 The Public Servants Disclosure Protection Act 2007 applies to wrongdoing in the "public sector", which is defined as government departments, public bodies and the federal public administration.[185] It specifically excludes from its remit the Canadian Forces, the Canadian Security Intelligence Service and the Communications Security Establishment.[186] Those responsible for each of these three excluded organisations must establish similar applicable procedures for the disclosure of wrongdoings, which specifically include protections for those who make disclosures concerning illegality or impropriety.[187]

A.152 The Governor in Council has the power to apply any provision of the Public Servants Disclosure Protection Act 2007 (subject to any modifications) to the three excluded organisations above.[188] Finally, in an effort to signal the protection of press freedoms, there is a provision which states that nothing in the Public Servants Disclosure Protection Act 2007 which relates to disclosures should be

[181] It should be noted that seven of the ten Canadian provinces have their own provincial public interest disclosure legislation. For an overview of these see Y Saint-Cyr, "The State of Whistleblowing Canada" (6 June 2013, *Slaw Magazine*) <http://www.slaw.ca/2013/06/06/the-state-of-whistleblowing-in-canada/> (last visited XXX) and M Forrest, "Yukon's whistleblower law comes into effect" (17 June 2015, *Yukon News*) <Available at: http://www.yukon-news.com/news/yukons-whistleblower-law-comes-into-effect/> (last visited 22 November 2016)

[182] Public Servants Disclosure Protection Act 2007, s 20.7(1).

[183] Public Servants Disclosure Protection Act 2007, s 5.1. Every chief executive shall establish a code of conduct applicable to the portion of the public sector for which he or she is responsible (Public Servants Disclosure Protection Act 2007, s 6.1.

[184] Public Servants Disclosure Protection Act 2007, s 6(1).

[185] Public Servants Disclosure Protection Act 2007 s 2(1). It draws upon the list departments named in Schedule I to the Financial Administration Act 1985.

[186] Public Servants Disclosure Protection Act 2007, s 2(1).

[187] Public Servants Disclosure Protection Act 2007, s 52.

[188] Public Servants Disclosure Protection Act 2007, s 53.

construed as applying to the dissemination of news and information by those employed by the Canadian Broadcasting Corporation.[189]

A.153 The Public Servants Disclosure Protection Act 2007 offers protection to disclosures which are classed as "wrongdoings in or relating to the public sectors".[190] There is a list of conduct which amounts to "wrongdoing" set out in section 8(a) to (f) of the Act:

(1) a breach of federal or provincial law;

(2) a misuse of public funds or a public asset;

(3) a gross mismanagement in the public sector;

(4) an act or omission that creates a substantial and specific danger to the life, health or safety of persons, or to the environment, other than a danger that is inherent in the performance of the duties or functions of a public servant; or

(5) a serious breach of the code of conduct set out in section 5 or 6 of the Public Servants Disclosure Protection Act 2007; and

(6) knowingly directing or counselling a person to commit a wrongdoing set out in any of paragraphs (1) to (5).

A.154 When a public servant (defined as an employee in the public sector) makes a disclosure of wrongdoing, they must ensure they do not provide more information than is reasonably necessary to make the disclosure and that they follow the established procedures for the secure handling, storage and transmission of information or documents.[191] Significantly, disclosures of wrongdoing cannot be made in respect of any information that is special operational information within the meaning of subsection 8(1) of the Security of Information Act 2001.[192]

A.155 Each government department must establish internal procedures to manage disclosures made under this Act by public servants.[193] A designated senior officer has responsibility for receiving and dealing with disclosures of wrongdoing, in accordance with the duties and powers of senior officers set out in the code of conduct established by the Treasury Board.[194]

A.156 Efforts must be made to protect the identity of the discloser, witnesses and those alleged to be responsible for wrongdoing.[195] The government department's chief executive must ensure that if wrongdoing is found to have taken place, there is

[189] Public Servants Disclosure Protection Act 2007, s 18.

[190] Public Servants Disclosure Protection Act 2007, s 8.

[191] Public Servants Disclosure Protection Act 2007, s 15(1)(a) and (b).

[192] Public Servants Disclosure Protection Act 2007, s 17.

[193] Public Servants Disclosure Protection Act 2007, s 10(1).

[194] Public Servants Disclosure Protection Act 2007, s 10(2).

[195] Public Servants Disclosure Protection Act 2007, s 11(1)(a).

prompt public access to information that describes the wrongdoing,[196] sets out the recommendations made in any report to the chief executive and what corrective action has been taken in response to the wrongdoing, and if no action has been taken, why this is the case.[197] However, this public access to information is subject to any statutory restrictions on the disclosure of information.[198]

A.157 There are three main ways of disclosing wrongdoing, or alleged wrongdoing, provided for by the Public Servants Disclosure Protection Act 2007:

(1) Disclosure to the employee's supervisor/senior officer.[199]

(2) Disclosure to the Public Sector Integrity Commissioner.[200]

(3) Disclosure to the public.[201] This is permitted only in strict circumstances. There must be insufficient time to make the disclosure to the supervisor or senior officer or the Commissioner *and* the public servant must have reasonable belief that the subject-matter of the disclosure constitutes a serious legal offence[202] or presents an imminent risk of a substantial and specific danger to the life, health and safety of persons or the environment.[203]

A.158 It should be noted that a number of exceptions apply to these disclosure provisions:

(1) None of these disclosure arrangements can be made with respect to any information that is special operational information per section 8(1) of the Security of Information Act 2001.[204]

(2) Disclosure to the public does not apply in relation to information which is subject to the legislative restrictions created by or under any Act of Parliament,[205] thus disclosures of information or material listed under the Security Information Act 2001 would be unlawful.

(3) Disclosures to the employee's supervisor or senior officer and the Commissioner are expressly qualified by the restrictions under section 18 of the Security of Information Act 2001: communication to a foreign entity

[196] Public Servants Disclosure Protection Act 2007, s 11(1)(c)(i).

[197] Public Servants Disclosure Protection Act 2007, s 11(1)(c)(ii).

[198] Public Servants Disclosure Protection Act 2007, s 11(2).

[199] Public Servants Disclosure Protection Act 2007, s 12.

[200] Public Servants Disclosure Protection Act 2007, s 13(1).

[201] Public Servants Disclosure Protection Act 2007, s 16(1).

[202] Public Servants Disclosure Protection Act 2007, s 16(1)(a).

[203] Public Servants Disclosure Protection Act 2007, s 16(1)(b) and s 42.3.

[204] Public Servants Disclosure Protection Act 2007, s 17.

[205] Public Servants Disclosure Protection Act 2007, s 16(1.1).

or to a terrorist group any information which the Government of Canada is taking measures to safeguard.[206]

A.159 It is an offence under the Public Servants Disclosure Protection Act 2007 for anyone knowingly to "take any reprisal" against a public servant, or to allow such action to take place.[207] There is a further prohibition which applies to non-public sector employer's,[208] making it an offence knowingly to take specific retaliatory measures against public servants that, in good faith and on the basis of reasonable belief, provide information or seek to do so, regarding alleged wrongdoing to the Commissioner.[209]

A.160 If found guilty of an offence, the sentence is a fine up of up to $10,000 and/or imprisonment for up to two years[210] or, on summary conviction, a fine up to $5,000 and/or imprisonment for up to six months.[211]

THE PUBLIC SERVICE INTEGRITY COMMISSIONER AND PUBLIC SERVANTS DISCLOSURE PROTECTION TRIBUNAL

A.161 The Public Service Integrity Commissioner ("the Commissioner") plays a central role in protecting public servants who disclose wrongdoing. The duties of the Commissioner include:

(1) Providing information and advice regarding the making of disclosures under the Public Servants Disclosure Protection Act 2007.[212]

(2) Receiving, recording and reviewing disclosures of wrongdoing in order to determine whether there are sufficient grounds for further action.[213]

(3) Conducting investigations into disclosures made to the Commissioner.[214]

(4) Ensuring that procedural fairness and natural justice are respected for all of those persons involved in investigations (including the person making the disclosure, but also the alleged wrongdoer).[215]

(5) Making recommendations to chief executives concerning the measures to be taken to correct wrongdoings and review reports on measures taken by chief executives in response to those recommendations.[216]

[206] Public Servants Disclosure Protection Act 2007, s 15(b).

[207] Public Servants Disclosure Protection Act 2007, s 19(1).

[208] Public Servants Disclosure Protection Act 2007, s 42.1(3).

[209] Public Servants Disclosure Protection Act 2007, s 42(1).

[210] Public Servants Disclosure Protection Act 2007, s 42(3)(a).

[211] Public Servants Disclosure Protection Act 2007, s 42(3)(b).

[212] Public Servants Disclosure Protection Act 2007, s 22(a).

[213] Public Servants Disclosure Protection Act 2007, s 22(b).

[214] Public Servants Disclosure Protection Act 2007, s 22(c).

[215] Public Servants Disclosure Protection Act 2007, s 22(d).

[216] Public Servants Disclosure Protection Act 2007, s 22(h).

A.162 A current or former public servant who has reasonable grounds for believing that they have suffered a reprisal for disclosing wrongdoing may file a complaint with the Commissioner[217] within 60 days of the reprisal being taken.[218] The Commissioner has the discretion to refuse to deal with a complaint if they are of the opinion that:

(1) the complaint has been adequately dealt with already or could be more appropriately resolved through another legislative provision or collective agreement;[219]

(2) the complaint is beyond the Commissioner's jurisdiction;[220] or

(3) the complaint was not made in good faith.[221]

A.163 This decision must be made by the Commissioner within 15 days after the complaint is filed. It should be noted that the filing of a complaint to the Commissioner precludes the complainant from commencing any other legislative procedure or collective agreement regarding the alleged reprisal.[222] This preclusion ceases to apply if the Commissioner decides not to deal with the complainant,[223] but, significantly, remains in place if the Commissioner's reason for not dealing with the complaint was that it was not made in good faith.[224]

A.164 If the outcome is not intended to address the complaint, this must be communicated to the complainant along with the reasons for the decision.[225] If the decision is made to investigate the complaint, investigations must be conducted as informally and expeditiously as possible,[226] with the aim of bringing wrongdoings to the attention of chief executives and making recommendations on corrective measures to be taken by them.[227] The Commissioner has the power to designate an investigator to investigate the complaint,[228] who must then submit

[217] Public Servants Disclosure Protection Act 2007, s 19(1).

[218] Public Servants Disclosure Protection Act 2007, s 19.1(3). This time period may be extended if the Commissioner feels it is appropriate given the circumstances of the complaint.

[219] Public Servants Disclosure Protection Act 2007, s 19.3(1)(a).

[220] Public Servants Disclosure Protection Act 2007, s 19.3(1)(c).

[221] Public Servants Disclosure Protection Act 2007, s 19.3(1)(d).

[222] Public Servants Disclosure Protection Act 2007, s 19.1(4).

[223] Public Servants Disclosure Protection Act 2007, s 19.4(4).

[224] Public Servants Disclosure Protection Act 2007, s 19.4(5).

[225] Public Servants Disclosure Protection Act 2007, s 19.4(3).

[226] Public Servants Disclosure Protection Act 2007, s 19.7(2).

[227] Public Servants Disclosure Protection Act 2007, s 26(1).

[228] Public Servants Disclosure Protection Act 2007, s 19.7(1).

their report of their findings to the Commissioner.[229] The Commissioner has the power to:[230]

(1) Obtain any facilities, assistance, information and office access from the relevant department as required to conduct the investigation (this power extends to the Commissioner's investigator too).[231]

(2) Subpoena witnesses and other powers contained in the Inquiries Act 1985.[232]

(3) Appoint a conciliator in an attempt to bring about a settlement.[233]

(4) Approve or reject the terms of any settlement agreed to by the complainant and the public sector employer.[234]

A.165 If, during the investigation, the Commissioner has reason to believe that another wrongdoing has been committed, the Commissioner may commence an investigation into the wrongdoing if they believe on reasonable grounds that the public interest requires an investigation.[235]

A.166 After receiving the investigator's report, the Commissioner must review the results of the investigation and report their findings to persons who made the disclosures and to the appropriate chief executives.[236] The Commissioner must then decide either to dismiss the complaint[237] or apply to the Public Servants Disclosure Protection Tribunal for a determination of whether or not a reprisal was taken against the complainant.[238]

A.167 In deciding whether to exercise this power, the Commissioner must take into account a number of criteria, including whether there are reasonable grounds for believing that a reprisal was taken against the complainant.[239] However, the

[229] Public Servants Disclosure Protection Act 2007, s 20.3.

[230] It should be noted that the Commissioner can delegate *any* of their powers under the Public Servants Disclosure Protection Act 2007 to any employee under section 25(1). Given how far-reaching these powers are, this seems a significant provision. However, the Commissioner may not delegate an investigation that involves or may involve information relating to international relations, national defence, national security or the detection, prevention or suppression of criminal, subversive or hostile activities, except to one of a maximum of four officers or employees of the Office of the Public Sector Integrity Commissioner specifically designated by the Commissioner for the purpose of conducting those investigations under section 25(2).

[231] Public Servants Disclosure Protection Act 2007, s 28(1). In exercising this provision though, the Commissioner must consider whether doing so will unduly disrupt the gathering and dissemination of news and information by the Corporation.

[232] Public Servants Disclosure Protection Act 2007, s 29(1).

[233] Public Servants Disclosure Protection Act 2007, s 20(2).

[234] Public Servants Disclosure Protection Act 2007, s 20.2(1).

[235] Public Servants Disclosure Protection Act 2007, s 33(1).

[236] Public Servants Disclosure Protection Act 2007, s 22(g).

[237] Public Servants Disclosure Protection Act 2007, s 20.5.

[238] Public Servants Disclosure Protection Act 2007, s 20.4(1).

[239] Public Servants Disclosure Protection Act 2007, s 20.4(3)(a) to (d).

Commissioner retains considerable discretion to refuse or cease an investigation on the grounds that they believe the subject-matter of the disclosure or the investigation is not sufficiently important,[240] or simply that there is a valid reason for not dealing with the subject-matter of the disclosure or investigation.[241]

A.168 If an application is made by the Commissioner to the Tribunal, a member of the Tribunal must be assigned to the case (up to three members may be assigned if the case is particularly complex). The Tribunal is an ad hoc body, made up of judges of the Canadian Federal Court or a superior court of a province.[242] It is the task of the Tribunal to determine whether the complainant has been subject to a reprisal and whether the person or persons identified by the Commissioner actually took the reprisal. It enjoys extensive powers, including:

(1) to summon and enforce the attendance of witnesses and compel them to give oral or written evidence on oath;

(2) to produce any documents and things that the member or panel considers necessary for the full hearing and consideration of the application; and

(3) to decide any procedural or evidentiary question.

A.169 Whilst the Public Servants Disclosure Protection Act 2007 states that proceedings are to be conducted as informally and expeditiously as the requirements of natural justice and the rules of procedure allow, there are provisions for legal advice to be made available to those involved in the investigation by Commissioner in certain circumstances.[243]

A.170 If the Tribunal determines that a reprisal was taken, it may, regardless of whether or not it has determined that the reprisal was taken by the person or persons in the application, make an order granting a remedy to the complainant and disciplinary action to be taken.[244] The remedies that the Tribunal may order are

[240] Public Servants Disclosure Protection Act 2007, s 24(1)(b).

[241] Public Servants Disclosure Protection Act 2007, s 24(1)(f).

[242] For an outline of the interlocutory decisions that have been handed down by the Public Servants Disclosure Protection Tribunal see Public Servants Disclosure Protection Tribunal Canada, *Historical Overview of Public Sector Whistleblower Protection* (January 2015) <http://publications.gc.ca/site/archivee-archived.html?url=http://publications.gc.ca/collections/collection_2015/tpfdc-psdptc/PE2-4-2015-eng.pdf> (last visited on 22 November 2016). See, in particular, *El-Helou v Courts Administration Service*, 2011 CanLII 93945 (CA PSDPT) in which the Tribunal held that Parliament clearly intended that the Commissioner perform a screening function to determine whether an application to the Tribunal is warranted and the Tribunal cannot, on its own initiative, bypass this role.

[243] Public Servants Disclosure Protection Act 2007, s 25.1(1). Noteworthy is that legal advice may only be provided if the Commissioner is of the opinion that the act or omission to which the disclosure or the information relates, likely constitutes a wrongdoing under this Act and that the disclosure or the provision of the information is likely to lead to an investigation being conducted under this Act (Public Servants Disclosure Protection Act 2007, s 25.1(3)).

[244] Public Servants Disclosure Protection Act 2007, s 21.5(5).

set out in the Act and range from permitting the complainant to return to their duties to up to $10,000 compensation.[245]

A.171 In addition, if the Tribunal determines that a reprisal was taken, the Commissioner may apply for an order for a remedy in favour of the complainant[246] and/or an order for disciplinary action against the person identified by the commissioner as having taken the reprisal.[247] If the decision is made to take disciplinary action, which can include termination of employment, the Tribunal must take into account a series of factors listed in the Public Servants Disclosure Protection Act 2007,[248] including the gravity of the reprisal and the deterrent effect of the disciplinary action.

The Canadian Criminal Code – section 425.1

A.172 It is a criminal offence under the Canadian Criminal Code to threaten or retaliate against employees. The conduct element is taking, or threatening to take, a disciplinary measure against, demote, terminate or otherwise adversely affect a person's employment.[249] This offence can be committed by either a person's direct employer or a person acting on behalf of an employer or in a position of authority in respect of an employee of the employer.[250] The fault element is:

(1) an intent to compel the employee from abstaining from providing information to a person whose duties include the enforcement of federal or provincial law, with respect to an offence that the employee believes has been or is being committed contrary to federal or provincial law;[251] or

(2) an intent to retaliate against an employee because they have provided such information.[252] Those found guilty of this offence are liable to imprisonment for up to five years.[253]

[245] Public Servants Disclosure Protection Act 2007, s 21.7(1).

[246] Public Servants Disclosure Protection Act 2007, s 20.4(1)(a).

[247] Public Servants Disclosure Protection Act 2007, s 20.4(1)(b).

[248] Public Servants Disclosure Protection Act 2007, s 21.8(1). It should be noted that the Tribunal must also take into account the extent to which inadequate disciplinary action might have an adverse effect on confidence in public institutions (Public Servants Disclosure Protection Act 2007, s 21.8(3)(b)).

[249] Canadian Criminal Code, s 425.1(1).

[250] Canadian Criminal Code, s 425.1(1).

[251] Canadian Criminal Code, s 425.1(1)(a).

[252] Canadian Criminal Code, s 425.1(1)(b).

[253] Canadian Criminal Code, s 425.1(2)(a).

AUSTRALIA

A.173 This section will first outline unauthorised disclosure and espionage offences contained in the Australian Criminal Code and a number of other statutes. This will be followed by discussion of the Australian Law Commission's report entitled "Secrecy Laws and Open Government in Australia". The section will then outline the mechanisms that allow for the protected disclosure of official information.

Criminal offences for committing unauthorised disclosures

A.174 The criminal offences governing disclosure of protected information in Australia have attracted attention in the last decade or so. The treason and espionage offences were remodeled in the aftermath of the 9/11 terrorist attacks, whilst other offences relating to disclosures at immigration detention centres were introduced as recently as 2015. [254]

A.175 In a report formidable in its size and scope of inquiry, the Australia Law Reform Commission identified 506 secrecy provisions in 176 pieces of legislation, including 358 distinct criminal offences on the federal statute books.[255] Further still, many Australian territories have similar offences containing broadly framed offences for the unauthorised disclosure of information by public officials.[256] The focus here is limited to the main federal criminal offences relating to persons who make unauthorised disclosures of protected information.

A.176 This part will outline offences that criminalise unauthorised disclosure and espionage activity within the following statutes:

(1) The Australian Criminal Code.

(2) The Crimes Act 1914.

(3) The Intelligence Services Act 2001.

(4) The Australian Security Intelligence Organisation 1979.

(5) The Australian Border Force Act 2015.

[254] See, for example, P Farrell, "Journalists Reporting on Asylum Seekers Referred to Australian Police" (22 January 2015, *The Guardian*) <https://www.theguardian.com/australia-news/2015/jan/22/journalists-reporting-on-asylum-seekers-referred-to-australian-police> (last visited 22 November 2016); George Newhouse, "Let Me Clear Up the Government's Clarification of the Border Force Act" (8 July 2015, *The Guardian*) <https://www.theguardian.com/commentisfree/2015/jul/08/let-me-clear-up-the-governments-clarification-about-the-border-force-act> (last visited 22 November 2016); and T Conboy, "Backing The Whistleblowers: Politics, Australia's Secrecy Laws And Our Criminal Justice System" (9 June 2015, *Newmatilda.com*) <https://newmatilda.com/2016/06/09/backing-the-whistleblowers-politics-australias-secrecy-laws-and-our-criminal-justice-system> (last visited 22 November 2016).

[255] For a discussion of their commonalities see: Australia Law Reform Commission, *Secrecy Laws and Open Government in Australia*, (December 2009) Report 112) Appendix 5.

[256] See Australia Law Reform Commission, *Secrecy Laws and Open Government in Australia* (December 2009) Report 112, p 88.

Section 91.1 of the Australian Criminal Code – Espionage

A.177 There are two main types of federal offence relating to espionage under section 91.1 of the Criminal Code, updated after 9/11. These offences relate to "information" concerning the "security or defence" of the Commonwealth or of another country (in the latter case, the information being acquired from the Commonwealth). "Information" refers to "information of any kind, whether true or false and whether in a material form or not", including an opinion and report of a conversation.[257] "Security or defence" includes the "operations, capabilities and technologies of, and methods and sources used by, the country's intelligence or security agencies".[258]

A.178 Section 91.1(1) to (2) prohibits communicating, or making available security or defence information, which results in, or is likely to result in the information being communicated, or made available, to another country or a foreign organisation (or person acting on their behalf). There are two offences based on this conduct, differing slightly in their fault element:

(1) Section 91.1(1) prohibits communicating, or making available, security or defence information with the intention to prejudice the Commonwealth's security or defence.

(2) Section 91.1(2) prohibits communicating, or making available, security or defence information without lawful authority and intending to give advantage to another country's security or defence. The penalty for both offences is 25 years' imprisonment.[259]

A.179 Section 91.1(3) to (4) prohibits making, obtaining or copying a record of security or defence information. Again, there are two offences based on this conduct, varying in their fault element requirements:

(1) Section 91.1(3)(b) requires an intention that:

   (a) the information will, or may, be delivered to another country or foreign organisation (or person acting on their behalf); and

   (b) it will prejudice the Commonwealth's security or defence.

(2) Section 91.1(4)(b) prohibits obtaining or copying a record:

   (a) without lawful authority; and

   (b) intending that it may, or will, be delivered to another country or foreign organisation (or person acting on their behalf); and

   (c) intending to give an advantage to another country's security or defence.

[257] Criminal Code Act 1995, s 90.1(1).

[258] Criminal Code Act 1995, s 90.1(1).

[259] Before the statutory amendments made after 9/11, imprisonment for both of these espionage offences was up to 7, not 25, years. See Explanatory Memorandum, Criminal Code Amendment (Espionage and Related Offences) Bill 2002 Sch 1.

A.180 Under section 91.2, it is a defence for the information the person communicates/makes available or makes/obtains/copies is information that is already available to the public with the authority of the commonwealth.[260]

Section 80 of the Australian Criminal Code (as amended by National Security Legislation Amendment Act 2010) schedule 1 – Treason

A.181 Section 80.1AA provides a separate offence for materially assisting the enemy. The conduct element is any conduct that assists the enemy, country or organisation.[261] The fault element is an intention to "materially assist" an enemy at war with the Commonwealth or a country or organisation that is engaged in armed hostilities with the Australian Defence Force.[262] The maximum available sentence is life imprisonment.

A.182 Hardy and Williams suggest that a person who releases information about Australia's military defences to a foreign security and intelligence agency for the purpose of instigating an armed invasion of Australia could be subject to prosecution under section 80.1. Most likely, though, the conduct would fall within section 80.1AA of materially assisting the enemy, especially if the person expected that a terrorist organisation would come into possession of the leaked information.[263]

A.183 Section 80.3 provides a defence to the offence of materially assisting the enemy (but not for the basic offence of treason) for acts done in good faith. The defence will be made out where the person "tries in good faith" to show that the Sovereign, Governor-General or Prime Minister is "mistaken in any of his or her counsels, policies or actions". In considering such a defence, the court may consider whether the acts were done for purposes "intended to be prejudicial to the safety or defence of the Commonwealth", or "with the intention of causing violence or creating public disorder or a public disturbance".

Crimes Act 1914 section 70 – Disclosure of information by Commonwealth officers

A.184 It is an offence under section 70 for current[264] or former[265] Commonwealth officers to publish or communicate, without authorisation, any fact or document which comes to their knowledge or possession by virtue of their employment, and which it is their duty not to disclose.[266]

[260] Criminal Code, s 91.2.

[261] Criminal Code, s 80.1AA(1)(d), (4)(c).

[262] Criminal Code, s 80.1AA(1)(e), (4)(d).

[263] K Hardy and G Williams, "Terrorist Traitor or Whistleblower? Offences and Protections in Australia for Disclosing National Security Information" (2014) 37(2) *UNSW Law Journal* 784, p 797.

[264] Crimes Act 1914, s 70(1).

[265] Crimes Act 1914, s 70(2).

[266] For a short list of some of the high profile, successful prosecutions under s 70 see Australia Law Reform Commission, *Secrecy Laws and Open Government in Australia* (December 2009) Report 112, p 88.

A.185 The offence does not create a standalone duty to keep information secret; the source of the duty must be found elsewhere, such as the common law, a specific secrecy provision or the terms of a contract.[267]

A.186 The offence covers a "Commonwealth officer" which, for the purposes of section 70, is defined in section 3 of the Crimes Act to include:

(1) a person appointed or engaged under the Public Services Act;

(2) a person employed in the public service of a territory, Australia Defence Force, Australian Federal Police or public authority under the Commonwealth;

(3) a person who performs services for or on behalf of the Commonwealth, a territory or public authority; and

(4) a person who performs services, or is an employee of the Australian Postal Corporation.

It should be emphasised that this is not an exhaustive list. By way of example, staff members of the Australian Secret Intelligence Service are now deemed "Commonwealth officers".[268]

A.187 Turning to the information covered, the term "any fact or document" is broad and could be construed as applying to the disclosure of any information regardless of its nature or sensitivity. Commentary on section 70 has highlighted this lack of clarity. For example, Tsaknis notes that it is unclear whether the release of any information would count as a "fact" or whether the information itself must be factually accurate.[269]

A.188 As to the activities covered, the definition of "publishes or communicates" is provided by the New South Wales Court of Appeal in *Kessing v The Queen*:

> To 'communicate' is to transmit or to impart knowledge or make known (Macquarie Concise Dictionary, 3rd ed). One may "communicate" a document by communicating the contents of the document. This is how the Crown particularised this case. Generally, 'to publish' connotes to make publicly known, however, in the law of defamation publication applies to making the matter complained of known to any person other than the person defamed.[270]

[267] Australia Law Reform Commission, *Secrecy Laws and Open Government in Australia,* (December 2009) Report 112, pp 88 and 95. In the case of *DPP v G* (1999) 85 FCR 566 the Federal Court held that a contractual obligation may be sufficient to constitute a duty under the former section 72 of the Crimes Act.

[268] By virtue of Intelligence Services Act 2001, s 38.

[269] L Tsaknis, "Commonwealth Secrecy Provisions: Time for Reform?" (1994) 18 *Criminal Law Journal* 254, p 261 as cited in *Commissioner of Taxation v Swiss Aluminium Australia Ltd* (1986) 10 FCR 321, p 325. See also P Finn, *Official Information, Integrity in Government Project: Interim Report 1* (1991), p 216 in Australia Law Reform Commission, *Secrecy Laws and Open Government in Australia* (December 2009) Report 112, p 91.

[270] *Kessing v The Queen* [2008] NSWCCA 310 at [31], by Bell JA.

A.189 The judgment in *Kessing v The Queen,* given by Judge Bell*,* also affirmed that communication of a document may be direct or indirect:

> This may be done directly by handing the document to another or by reading the document to another. It may be done indirectly by leaving the document on a park bench for another to collect or in any of a variety of ways.[271]

Crimes Act 1914 section 79 – Disclosure of official secrets

A.190 Section 79 of the Crimes Act creates a number of offences that relate to the use or disclosure of official secrets. Unlike section 70, offences prosecuted under section 79 require the consent of the Attorney-General[272] because they are likely to raise issues regarding matters of national security or sensitive international relations that require government to government contact.[273]

A.191 By way of background, an earlier version of this provision appeared in the Crimes Act 1914, based on the United Kingdom's Official Secrets Act 1911. The Criminal Code Amendment (Espionage and Related Offences) Bill 2002 was originally intended to repeal and replace section 79 with updated provisions in the Criminal Code*.* Among other things*,* the Bill provided for sentences of imprisonment for secondary disclosure in relation to non-national security matters, even when the information was disclosed or published on so-called public interest grounds.[274]

A.192 The provisions were criticised for their potential impact on freedom of speech and public discussion of important issues of public interest, and ultimately they were replaced.[275] Aside from a minor amendment, section 79 remains in place as the federal offence relating to the disclosure of official secrets.[276]

A.193 Section 79 applies to:

(1) commonwealth officers (current and former);[277]

[271] *Kessing v The Queen* [2008] NSWCCA 310 at [36], by Bell JA, as cited in Australia Law Reform Commission, *Secrecy Laws and Open Government in Australia,* Report 112, December 2009, p91.

[272] Crimes Act 1914, s 85.

[273] Australia Law Reform Commission, *Secrecy Laws and Open Government in Australia* (December 2009) Report 112, p 264.

[274] See Parliament of Australia, "The Criminal Code Amendment (Espionage and Related Offences) Bill 2002" <http://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/bd/bd0102/02bd117> (last 22 November 2016).

[275] See Australia Law Reform Commission, *Secrecy Laws and Open Government in Australia* (December 2009) Report 112, p 94.

[276] The amendment replaces the term "[intention to prejudice the] safety or defence" with that of "[intention to prejudice the] security or defence. The Federal Government has stated that the objective behind this was to protection to a wider range of material. See Parliament of Australia, "The Criminal Code Amendment (Espionage and Related Offences) Bill 2002" <http://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/bd/bd0102/02bd117> (last visited 22 November 2016).

[277] Crimes Act 1914, s 79(1)(b)(i). The definition of "Commonwealth officer" is found in section 3 of the Crimes Act, as discussed above in relation to section 70.

(2) those who hold, or have held, an office under the Queen;[278]

(3) those who have, or have held, a contract made on behalf of the Commonwealth;[279]

(4) those acting with the permission of a Minister;[280] and

(5) those who have been entrusted with official secrets information by a Commonwealth officer.

In summary, the offences apply to both initial disclosures by those holding such information by virtue of their work (most obviously, Commonwealth officers), as well as secondary disclosures by third parties.

A.194 The offence applies to prescribed information under section 79 which can take the form of a "sketch, plan, photograph, model, cipher, note, document or article". The terms are broadly defined: "Article" refers to "any thing, substance or material" and information means "information of any kind whatsoever, whether true or false and whether in a material form or not and includes an opinion and a report of a conversation".[281] This information must be in the person's possession or control.[282]

A.195 There are three classes of information which are protected, the first two of which relate to specific types information, while the third is more general in application:

(1) Information that is made or obtained in contravention of Part VI of the Crimes Act or section 91.1 of the Criminal Code (espionage provision).[283]

(2) Information that relates to a prohibited place or anything inside it, and which the person knows or ought to know that it should not be communicated to an unauthorised person.[284]

(3) Information entrusted to a Commonwealth officer, Commonwealth contractor, or person acting with the permission of a minister; or entrusted to a person by a Commonwealth officer, and, owing to the nature/circumstances under which it was entrusted to the person, it is the person's duty to treat it as secret.[285]

A.196 Section 79 creates five offences relating to the use and disclosure of the prescribed information described above:

[278] Crimes Act 1914, s 79(1)(b)(ii).

[279] Crimes Act 1914, s 79(1)(b)(iii).

[280] Crimes Act 1914, s 79(1)(b)(v).

[281] Crimes Act 1914, s 79(1).

[282] Crimes Act 1914 s 79(1).

[283] Crimes Act 1914, s 79(1)(a).

[284] Crimes Act 1914, s 79(1)(c).

[285] Crimes Act 1914, s 79(1)(b).

(1) Section 79(2) – communicating, retaining or allowing someone access to prescribed information without authorisation. This offence has the fault element of an intention to prejudice the security or defence of the Commonwealth. The maximum sentence available is 7 years' imprisonment. An exception is provided where it is the person's duty to communicate the information in the "interest of the Commonwealth". The corresponding exception in the Official Secrets Act 1911, which this provision is based on, was held to refer to an official duty, rather than a moral, contractual or civic duty, while the "interests of state" were interests according to its recognised organs of government.

(1) Section 79(3) – communicating or allowing someone to access prescribed information without authorisation. The maximum sentence available is 2 years' imprisonment. The exception mentioned under section 79(2) – based on the "interest of the Commonwealth – also applies to section 79(3).

(2) Section 79(4) – retaining prescribed information, failing to comply with a direction given by lawful authority with respect to prescribed information or failing to take care of prescribed information or behaving in a way that could endanger the safety of the information. The maximum sentence available is six months' imprisonment.

(3) Section 79(5) – receiving prescribed information, knowing or having reasonable grounds to belief, that when the information was communicated to him or her, it was done so in contravention of section 79(2) Crimes Act or section 91.1 of the Criminal Code (the espionage offence). An offence is not committed if the person can prove that the communication was contrary to his or her desire. The maximum sentence available is 7 years' imprisonment.

(4) Section 79(6) – receiving prescribed information knowing or having reasonable grounds to belief, that when the information was communicated to him or her, it was done so in contravention of section 79(3) Crimes Act. An offence is not committed if the person can prove that the communication was contrary to his or her desire. The maximum sentence available is 2 years' imprisonment.

A.197 It should be emphasised that section 79 applies to prescribed information regardless of the effect of its disclosure: there is no requirement for harm to have been caused by the information being disclosed.[286] While both section 91.1 of the Criminal Code and section 79 of the Crimes Act both cover conduct involving disclosure, retention and copying protected information concerning the security or defence of the Commonwealth, section 91.1 is distinct in that the requisite element of the offence is that the information be communicated, or intended to be communicated, to another country or organisation.[287]

[286] For further discussion, see Australia Law Reform Commission, *Secrecy Laws and Open Government in Australia* (December 2009) Report 112, p 96.

[287] For further discussion see Australia Law Reform Commission, *Secrecy Laws and Open Government in Australia* (December 2009) Report 112, p 320.

A.198 By way of summary, both section 70 and section 79(3) are broadly drafted provisions and share a degree of overlap: they apply to a similar, broad range of information, regarding a breach of a "duty" that is found either outside the criminal provision of their particular Act or determined by the nature of the information or the circumstances of the communication. However, section 79 extends beyond Commonwealth officers to include other persons described in section 79(1)(a) to (c). Unlike section 70, there is an exception provided in section 79(3)(b) that allows communication of information "in the interests of the Commonwealth".[288]

A.199 The Australian Law Reform Commission reported that since 2000 the majority of prosecutions for the breach of secrecy provisions have been brought under section 70, even where specific secrecy offence would have been available. There have been only a few prosecutions under section 79. One recent example is the conviction in 2003 of an employee of the Defence Intelligence Organisation, Simon Lappas, under section 79(3), for disclosing several classified documents to an unauthorised person, so they could be sold to a foreign country. Lappas was found guilty and sentenced to 2 years' imprisonment.[289]

Intelligence Services Act 2001 – Disclosure by employees of intelligence organisations

A.200 Sections 18, 39, 39A and 40 of the Intelligence Services Act 2001 establish offences for employees of the Australian Security Intelligence Organisation, the Australian Secret Intelligence Service, the Defence Imagery and Geospatial Organisation and the Australian Signals Directorate respectively.

A.201 Under these provisions, it is an offence, punishable up to a maximum of 2 years' imprisonment and/or a fine, where an employee of the intelligence agency:

> Communicates any information or matter that was prepared by or on behalf of [the agency] in connection with its functions, or relates to the performance by [the agency] of its functions.

A.202 These offences apply regardless of the type of information communicated by the person or any intention on behalf of the person to prejudice security or defence.

[288] For further comment, see Australia Law Reform Commission, *Secrecy Laws and Open Government in Australia* (December 2009) Report 112, p 98.

[289] Australia Law Reform Commission, *Secrecy Laws and Open Government in Australia* (December 2009) Report 112, p 94.

Australian Security Intelligence Organisation Act 1979 (as amended by National Security Legislation Amendment Act (No. 1) (2014)) – Special intelligence operations

A.203 The National Security Legislation Amendment Act (No. 1)(2014) established a "special intelligence operation" scheme under which Australian Security Intelligence Organisation officers and affiliates are protected from criminal and civil liability for certain conduct engaged in for the purpose of a special intelligence operation. Included in this amendment to the Australian Security Intelligence Organization Act 1979 was the introduction of two new offences for authorised disclosure of information relating to special intelligence operations, in order to "protect persons participating in a special intelligence operation and to ensure the integrity of operations".[290]

A.204 The first offence, under section 35P(1) of the Australian Security Intelligence Organization Act 1979, occurs where a person discloses information and the information relates to a special intelligence operation. The maximum available penalty is imprisonment for 5 years. The provision itself does not specify a fault element and, as a result, section 5.6 of the Criminal Code Act 1995 has effect: section 35P(1) must be read as requiring that a person intentionally disclosed information and the person was aware of a substantial risk that the information related to a special intelligence operation, and having regard to the circumstances known to him or her, it was unjustifiable to take the risk.

A.206 The second offence, under section 35P(2) of the Australian Security Intelligence Organization Act 1979*,* occurs where the person discloses information relating to a special intelligence operation and the person either:

(1) intends to endanger the health or safety of any person or prejudice the effective conduct of a special intelligence operation; or

(2) the disclosure of the information will endanger the health or safety of any person or prejudice the effective conduct of a special intelligence operation.

A.207 The maximum available penalty for this offence is 10 years' imprisonment.

[290] For further discussion of the legislation see Cat Barker, "Offences for Disclosing Information about Covert Operations: a Quick Guide" (23 October 2014, *Parliament of Australia*). <http://www.aph.gov.au/About_Parliament/Parliamentary_Departments/Parliamentary_Library/pubs/rp/rp1415/Quick_Guides/Offences> (last visited, 22 November 2016).

Australian Border Force Act 2015

A.208 The Australian Border Force Act 2015 applies to an "entrusted person" – that is, the Secretary; the Australian Border Force Commissioner; or an Immigration and Border Protection worker. An Immigration and Border Protection worker is defined very broadly in the Act to include an officer or employee of an Australian State or Territory and an officer or employee of the government of a foreign country or of a public international organisation whose services are made available to the Australian Border Force, as well as consultants or contractors for the Australian Border Force.[291]

A.209 It is an offence for an entrusted person to make a record of or disclose, protected information[292] unless the making of the record or disclosure is:

(1) authorised by the Act;

(2) is in the course of the person's employment or service as an entrusted person; or

(3) is required or authorised by law or by an order or direction of a court or tribunal.[293]

A.210 Further situations in which a disclosure may lawfully be made under the Act include the following.

(1) Disclosure to reduce threat to life or health, provided:

(a) the entrusted person reasonably believes that the disclosure is necessary to prevent or lessen a serious threat to the life or health of an individual; and

(b) the disclosure is for the purposes of preventing or lessening that threat.[294]

(2) Disclosure of publicly available information: an entrusted person may disclose protected information if it has already been lawfully made available to the public.[295]

(3) Disclosure for the purposes of the Law Enforcement Integrity Commissioner Act 2006 or regulations under that Act (corruption).[296]

Mechanisms that allow for the protected disclosure of official information

A.211 This section will examine the Public Interest Disclosure Act 2013, which is the federal legislation that governs the process for making protected disclosures. Whilst each state has its own state-specific legislation that provides for protected

[291] Australian Border Force Act 2015, s 4(1).

[292] Australian Border Force Act 2015, s 42(1)(a) to (c).

[293] Australian Border Force Act 2015, s 42(2).

[294] Australian Border Force Act 2015, s 48.

[295] Australian Border Force Act 2015, s 49.

[296] Australian Border Force Act 2015, s 43.

disclosures, these statutes are similar to the Public Interest Disclosure Act 2013 in regards to both the categories of information that are protected and the type of protection that is afforded to individuals.

The Public Interest Disclosure Act 2013

A.212 In several of its earlier reports, the Australian Law Reform Commission called on the Australian Government to introduce comprehensive public interest disclosure legislation encompassing all Australian Government agencies.[297] Likewise, the Standing Committee on Legal and Constitutional Affairs strongly recommended "as a matter of priority", the introduction of a comprehensive scheme for protecting those who make disclosures of illegality or impropriety at the national level.[298] Ultimately, this came in the form of the Public Interest Disclosure Act 2013.

A.213 The Act came into force in January 2014, with the aim of encouraging and facilitating the making of disclosures of wrongdoing by public officials, and ensuring that public officials who make protected disclosures are supported and protected from adverse consequences relating to the making of a disclosure.

A.214 To be able to make a disclosure under the Public Interest Disclosure Act 2013, a person must be a current or former "public official". This is defined in the Act to include a broad class of persons, including: a Commonwealth public servant, a member of the Defence Force, an appointee of the Australian Federal Police, the Australian Security Intelligence Organisation, and the Australian Secret Intelligence Service.[299] A person or organisation that provides goods or services under a Commonwealth contract and their officers or employees are included too.[300] It should also be noted that an authorised officer under the Act has the power to deem a person to be a public official if they reasonably believe the person has information about wrongdoing and proposes to make a disclosure.[301]

A.215 To constitute a public interest disclosure under the Public Interest Disclosure Act 2013, the type of information disclosed must fall within one of the following types of conduct:

(1) A breach of Commonwealth, a State or a Territory law or a corresponding law in a foreign country applicable to the relevant agency, public official or contracted service provider.

[297] Australian Law Reform Commission, *Keeping Secrets: The Protection of Classified and Security Sensitive Information*, ALRC 98 (2004), Recommendation 3–1; Australian Law Reform Commission, *Integrity: But Not by Trust Alone: AFP & NCA Complaints and Disciplinary Systems*, ALRC 82 (1996), Recommendation 117.

[298] House of Representatives Standing Committee on Legal and Constitutional Affairs, *Whistleblower Protection: A Comprehensive Scheme for the Commonwealth Public Sector* (February 2009, *Parliament of Australia*). It should be noted that Australia has separate whistleblowing legislation for each of its states. For example, the Whistleblowers Protection Act 1993 (South Australia), the Protected Disclosures Act 1994 (New South Wales), the Public Interest Disclosures Act 1994 (Australian Capital Territory), the Whistleblowers Protection Act 2001 (Victoria) and the Public Interest Disclosures Act 2003 (Western Australia).

[299] Public Interest Disclosure Act 2013, s 69(1)(a).

[300] Public Interest Disclosure Act 2013, s 30.

(2) Perverting or attempting to pervert the course of justice or conduct that involves corruption of any other kind; or that constitutes maladministration.

(3) An abuse of public trust.

(4) Fabrication, falsification, plagiarism, or deception, in relation to scientific research.

(5) The wastage of money or property of an authority under the Act.

(6) It unreasonably results in a danger, or risk of danger, to the health or safety of a person(s).

(7) A danger, or risk of danger, to the environment.[302]

(8) Conduct engaged in for the purpose of the public official abusing his or her position.

(9) Conduct engaged in by a public official that could give reasonable grounds for disciplinary action against the public official.[303]

A.216 This particular type of conduct must have been engaged in by:

(1) an agency;

(2) a public official in connection with his or her position as a public official; or

(3) a contracted service provider for a Commonwealth contract (in connection with that contract).[304]

A.217 The Public Interest Disclosure Act 2013 explicitly states that neither of the following are disclosable:

(1) Conduct which relates only to policy of the Commonwealth Government or the action of a Minister, Speaker of the House of Representatives or President of the Senate with which a person disagrees or expenditure related to such policy or action.[305]

(2) Conduct that an intelligence agency or a public official thereof engages in during the proper performance of its functions or exercise of its powers.[306]

[301] Public Interest Disclosure Act 2013, s70.

[302] Public Interest Disclosure Act 2013 s 29(1). Commonwealth Ombudsman, *Agency Guide to the Public Interest Disclosure Act 2013*, (December 2013) Version 1.

[303] Public Interest Disclosure Act 2013 s 29(2).

[304] Public Interest Disclosure Act 2013, s 29(1)(a) to (c).

[305] Public Interest Disclosure Act 2013, s 32.

[306] Public Interest Disclosure Act 2013, s 33.

If the above criteria are satisfied, then the person can be protected from civil, criminal or administrative liability; be protected from reprisal; apply for compensation; and can apply for a range of court orders. It is worth briefly expanding upon each of these protections.

A.218 The Act provides that a person who makes a public interest disclosure is not subject to any civil, criminal or administrative liability (including disciplinary action) for making the disclosure.[307] As explained by the Commonwealth Ombudsman, this means, for example, that a person would not be committing an offence under the Crimes Act 1914 if they made a disclosure in accordance with the Public Interest Disclosure Act 2013.[308]

A.219 If civil or criminal proceedings are instituted against someone because they made a disclosure, the discloser can claim immunity under section 10 of the Public Interest Disclosure Act 2013.[309] The discloser must be able to point to evidence that suggests a reasonable possibility that their claim to being exempt from liability is correct,[310] it is then a matter for the person bringing the proceedings against the discloser to prove that the claim is incorrect.[311]

A.220 No contractual or other remedy may be enforced, and no contractual or other right may be exercised, against a person on the basis of the public interest disclosure.[312] A contract to which the discloser is a party cannot be terminated because of the public interest disclosure.[313]

A.221 However, these immunities from liability no longer apply if the discloser knowingly makes a statement that is false or misleading[314] or makes a disclosure knowing that it contravenes a designated publication restriction and without a reasonable excuse for doing so.[315]

[307] Public Interest Disclosure Act 2013, s 10(1)(a).

[308] Commonwealth Ombudsman, *Agency Guide to the Public Interest Disclosure Act 2013*, (December 2013) Version 1, p 47.

[309] Public Interest Disclosure Act 2013, s 23.

[310] Public Interest Disclosure Act 2013, s 23(1)(a).

[311] Public Interest Disclosure Act 2013, 23(1)(b).

[312] Public Interest Disclosure Act 2013, s 10(1)(b).

[313] Public Interest Disclosure Act 2013 s 10(1)(b).

[314] Public Interest Disclosure Act 2013, s 11.

[315] Public Interest Disclosure Act 2013, s 11A.

A.222 Furthermore, taking a reprisal against a person who makes a public interest disclosure is a criminal offence, punishable by imprisonment for up to 2 years and/or a fine.[316] It is not necessary to prove that a person actually made or intended to make a public interest disclosure,[317] what is instead relevant is the intention and action of the person who took the reprisal. It is also an offence to threaten to take a reprisal and either intend the threat to cause fear or be to reckless toward this occurring.[318] It is not necessary to prove that the person who was threatened actually feared that the threat would be carried out.[319]

A.223 A reprisal occurs where someone causes, by an act or omission, any detriment to another person because they believe or suspect that person, or anyone else, may have made or intends to make a public interest disclosure.[320] "Detriment" includes any disadvantage to a person, including dismissal, injury in their employment, discrimination between them and other employees or alteration of their position to their disadvantage.[321] As suggested by the Commonwealth Ombudsman, further examples of detriment for the purposes of the Act might include:

(1) a physical or psychological injury, including a stress-related injury; intimidation, harassment or victimisation;

(2) loss or damage to property; or

(3) a disadvantage to a person's career (for example, denying them a reference or a promotion without appropriate reasons).[322]

A.224 A person also has the right to apply for compensation for loss, damage or injury suffered as a result of a reprisal or threat of reprisal.[323] A claim can be made not only against the person causing the reprisal but also their employer if the reprisal is in connection with their position as an employee.[324] The employer has a defence if they took reasonable precautions and exercised due diligence to avoid the reprisal or threat.[325]

[316] Public Interest Disclosure Act 2013, s 19.

[317] Public Interest Disclosure Act 2013, s 19(2).

[318] Public Interest Disclosure Act 2013, s 19(3).

[319] Public Interest Disclosure Act 2013, s 19(3).

[320] Public Interest Disclosure Act 2013, s 13(1).

[321] Public Interest Disclosure Act 2013, s 13(2).

[322] Commonwealth Ombudsman, *Agency Guide to the Public Interest Disclosure Act 2013*, (December 2013) Version 1, p 49.

[323] Public Interest Disclosure Act 2013, s 14.

[324] Public Interest Disclosure Act 2013, s 14(1).

[325] Public Interest Disclosure Act 2013, s 14(2).

A.225 Lastly, a person who has made a public interest disclosure can apply to the Federal Court or Federal Circuit Court for a range of orders where reprisal against them has been threatened or taken. A person has the right to take such action even if a prosecution for a reprisal offence has not been, or cannot be, brought.[326] Where the court is satisfied that another person took, threatened, or is taking or threatening, a reprisal, the court may grant an injunction: restraining that person from taking or threatening to take a reprisal; requiring the person to do something, including making an apology, or any other order the court considers appropriate.[327] The court may also order a person to be reinstated to their position, or a position at a comparable level, if satisfied that the person's employment was terminated wholly or partly as a reprisal for making or proposing to make a public interest disclosure.[328]

A.226 A disclosure must be made to an appropriate person in order to gain the protections available under the Act.[329] A public interest disclosure may be made orally or in writing.[330] Disclosers do not have to identify themselves and may remain anonymous.[331] A person making a disclosure does not need to assert that the disclosure is made under the Act for it to be a public interest disclosure and for the requirements of the Act to apply.[332] There are two main forms of authorised disclosure that can be made: internal and external.

A.227 Public officials can report suspected wrongdoing to their current supervisor in an agency, or to an "authorised officer" of their agency. The latter are the key figures with responsibilities for internal public interest disclosures under the Act. The term "authorised officers" encompasses agency heads, or "principal officers" of the relevant agency; and public officials either belonging to the agency or appointed by the principal officer.[333] Each agency must have procedures for dealing with public interest disclosures, and should set out in its procedures how a disclosure should be made.[334]

[326] Public Interest Disclosure Act 2013, s 19A.

[327] Public Interest Disclosure Act 2013,s 15.

[328] Public Interest Disclosure Act 2013, s 16.

[329] Public Interest Disclosure Act 2013, s 26. For a helpful overview of the procedure see Commonwealth Ombudsman, *Agency Guide to the Public Interest Disclosure Act 2013*, (December 2013) Version 1, p 30.

[330] Public Interest Disclosure Act 2013, s 28(1).

[331] Public Interest Disclosure Act 2013, s 28(2).

[332] Public Interest Disclosure Act 2013, s *28*(2).

[333] Public Interest Disclosure Act 2013, s 36.

[334] Public Interest Disclosure Act 2013, s 59.

A.228 A public official may make a disclosure to their "supervisor".[335] A supervisor includes any public official who supervises or manages the discloser.[336] Principal officers must establish procedures for facilitating and dealing with public interest disclosures relating to the agency.[337] These procedures must include assessing risks that reprisals may be taken against a person who makes a disclosure, and providing for confidentiality of investigative processes taking.[338]

A.229 The principal officer is responsible for conducting investigations of the alleged wrongdoing, but may delegate those powers and functions to an officer who belongs to their agency.[339] The principal officer must appoint in writing authorised officers to receive public interest disclosures.[340]

A.230 The authorised officers have a range of decision-making, notification and other responsibilities under the Public Interest Disclosure Act 2013. An individual may have decided to make a disclosure or may want to first seek advice about the process or the protections available to them, and an authorised officer should be prepared to explain what the Act requires.[341] If the supervisor or manager believes that the information given to them concerns, or could concern, disclosable conduct, they must give that information to an authorised officer of the agency as soon as reasonably practicable.[342]

A.231 Once a disclosure has been made, the first step of the authorised officer is to examine the information that has been supplied and decide whether it is an internal disclosure under the Public Interest Disclosure Act 2013.[343] The authorised officer has the power to make any inquiries and may obtain further information before making a decision about allocating the matter for investigation.[344] The authorised officer must allocate the matter for investigation, unless they are reasonably satisfied that there is no reasonable basis for considering the matter to be an internal disclosure.[345] The authorised officer must take this action within 14 days of becoming aware of the disclosure, unless there is a good reason why they need further time.[346]

[335] Public Interest Disclosure Act 2013, s 26.

[336] Public Interest Disclosure Act 2013, s 28.

[337] Public Interest Disclosure Act 2013, s 59(1).

[338] Public Interest Disclosure Act 2013, s 59(3)(a).

[339] Public Interest Disclosure Act 2013, s 77.

[340] Public Interest Disclosure Act 2013, s 36.

[341] Public Interest Disclosure Act 2013, s 60.

[342] Public Interest Disclosure Act 2013, s 60A.

[343] Public Interest Disclosure Act 2013, s 70.

[344] Public Interest Disclosure Act 2013, s 43(4).

[345] Public Interest Disclosure Act 2013, s 43(2).

[346] Public Interest Disclosure Act 2013, s 43(5).

A.232 An investigator who suspects that information disclosed as part of an internal disclosure, or information that is obtained during the course of an investigation, constitutes evidence of an offence against a Commonwealth, state or territory law, may disclose that information to a member of a relevant police force.[347] Depending on the particular offence involved, this could be a police force of a state or territory. However, in cases where the potential offence is serious (that is, punishable by imprisonment for 2 years or more), notification of the relevant police force is mandatory.[348]

A.233 The confidentiality of the person making the disclosure is something that is taken very seriously under the Public Interest Disclosure Act 2013 during the investigation of the disclosure. It is an offence for a person who has information obtained in the course of conducting a disclosure investigation to disclose or use the information.[349] The penalty is imprisonment for up to 2 years and/or a fine. No offence is committed, however, if the use of the information is for the purposes of the Act or in connection with the person's powers and functions under the Act or the information has previously been lawfully published and is not intelligence information, or if it is intelligence information, the principal officer of the source agency for the information has consented to the disclosure or use.[350] The discloser's identifying information must also not be disclosed to a court or tribunal except when necessary to give effect to the Act.[351]

A.234 The principal officer may decide not to investigate, or may discontinue an investigation, on the basis of a list of criteria set out in the Public Interest Disclosure Act 2013:

(1) the discloser is not a current or former public official;

(2) the information does not to any extent concern serious disclosable conduct;

(3) the disclosure is frivolous or vexatious;

(4) the disclosure is the same or substantially the same as another disclosure which has been or is being investigated under the Act or under another Commonwealth law;

(5) the principal officer is reasonably satisfied that there are no matters that warrant further investigation;

(6) the discloser has advised the principal officer that they do not wish the investigation to be pursued, and the principal officer is reasonably satisfied that there are no matters that warrant further investigation; or

(7) it is impracticable to investigate the disclosure because:

[347] Public Interest Disclosure Act 2013, s 56(1).

[348] Public Interest Disclosure Act 2013, s 56(2).

[349] Public Interest Disclosure Act 2013, s 65(1).

[350] Public Interest Disclosure Act 2013, s 65(2).

[351] Public Interest Disclosure Act 2013, s 21.

(i) of the age of the information;

(ii) the discloser has not revealed their name and contact details; or

(iii) the discloser has failed to or is unable to give the investigator the information or assistance they requested.[352]

A.235 Notice of a decision not to investigate must be given to the discloser, provided they are readily contactable.[353] The notice must give reasons for the decision and other action that may be available to them under other Commonwealth laws (such as in relation to a workplace grievance).[354] A principal officer who decides not to investigate an internal disclosure must also give their reasons to the Ombudsman, or to the Inspector General of Intelligence and Security in relation to the intelligence agencies.[355]

A.236 If an internal disclosure has been investigated, the Public Interest Disclosure Act 2013 requires all public officials to give their best endeavours to assist the principal officer in the conduct of an investigation.[356] After the investigation has taken place, the principal officer must prepare a report that sets out the matters considered, how long the investigation took, any findings that were made, any action either recommended or taken, any claims or evidence of detrimental action to the discloser, and the agency's response to those claims.[357] The principal officer must give a copy of the investigation report to the discloser within a reasonable time of preparing it; provided that it is reasonably practical to contact the discloser.[358]

A.237 A public official can also make a disclosure to authorised officers of the Commonwealth Ombudsman, if they believe on reasonable grounds that it would be appropriate for the Ombudsman to investigate it.[359] If the matter involves an intelligence agency or intelligence-related information, a public official can make a disclosure to the intelligence agency, or to an authorised officer of the Inspector General of Intelligence and Security if they believe on reasonable grounds that it would be appropriate for the Inspector General of Intelligence and Security to investigate.[360]

[352] Public Interest Disclosure Act 2013, s 48.

[353] Public Interest Disclosure Act 2013, s 50.

[354] Public Interest Disclosure Act 2013, s 50(2).

[355] Public Interest Disclosure Act 2013, s 50(A).

[356] Public Interest Disclosure Act 2013, s 61(1).

[357] Public Interest Disclosure Act 2013, s 51.

[358] Public Interest Disclosure Act 2013, s 51(4).

[359] Public Interest Disclosure Act 2013, s 26(1).

[360] Public Interest Disclosure Act 2013, s 34(1).

A.238 The Ombudsman will consider whether special reasons exist to conduct an investigation, or allocate the matter to the agency where the disclosable conduct is alleged to have occurred, or to a prescribed investigative agency with appropriate jurisdiction. The Inspector General of Intelligence and Security will become involved in an investigation in similar circumstances to those of the Ombudsman, but in respect of matters relating to the intelligence agencies.

A.239 A public official who has already made an internal disclosure under the Act may make a disclosure to any person if any of the following criteria are met:

(1) The internal investigation under the Act was not completed (meaning that the report of investigation was not finalised) within ninety days.

(2) They believe on reasonable grounds that the investigation under the Act was inadequate.

(3) They believe on reasonable grounds that the agency took inadequate action after the investigation was completed.

(4) It is not contrary to the public interest for an external disclosure to be made.[361]

A.240 The Public Interest Disclosure Act 2013 sets out a number of broad-termed factors that must be taken into account in determining that a disclosure is not contrary to the public interest. These include:

(1) the extent to which the disclosure would expose a failure to address serious wrongdoing;

(2) the nature and seriousness of the disclosable conduct;

(3) any risk that disclosure could prejudice the proper administration of justice;

(4) the principle that disclosures should be properly investigated and dealt with; and

(5) any other relevant matter.[362]

A.241 External disclosures by a public official are subject to two further qualifications:

(1) No more information should be publicly disclosed than is reasonably necessary to identify one or more instances of disclosable conduct.[363]

(2) The information must not consist of, or include, intelligence information or relate to an intelligence agency.[364]

[361] Public Interest Disclosure Act 2013, s 26(1) item 2.

[362] Public Interest Disclosure Act 2013, s 26(3).

[363] Public Interest Disclosure Act 2013, s 26(1) item 2(f).

[364] Public Interest Disclosure Act 2013, s 26(1) item 2(h). (Intelligence information being defined in Public Interest Disclosure Act 2013, s 41).

A.242 Intelligence information is defined broadly to include information that has originated with or been received from an intelligence agency or is sensitive law enforcement information.[365]

A.243 If a public official believes, on reasonable grounds, that the information they wish to disclose concerns a substantial and imminent danger to the health or safety of one or more people or to the environment, they may make an emergency disclosure to anyone, provided the following criteria are met:

(1) the extent of the information disclosed must be only what is necessary to alert the recipient of the substantial and imminent danger;

(2) if there has not been an internal disclosure about the matter, or if the investigation is not yet completed, there must be exceptional circumstances justifying the disclosure; and

(3) as noted above, the disclosure must not relate to intelligence information, including sensitive law enforcement information.[366]

NEW ZEALAND

A.244 This section will first outline unauthorised disclosure and espionage offences contained in statute. This discussion will then be followed by an outline of the mechanisms that allow for the protected disclosure of official information and briefly examine a number of issues arising under the current law. Both of these sections will include discussion of the New Zealand Intelligence and Security Bill, which is currently before the New Zealand Parliament. The Bill proposes additional disclosure offences and further safeguards to current disclosure mechanisms.

Criminal offences for unauthorised disclosures

A.245 This section will examine criminal offences governing the unauthorised disclosure of protected information in the following statutes:

(1) The Crimes Act 1961.

(2) The Summary Offences Act 1981.

(3) The Security Intelligence Service Act 1969.

A.246 This section will also outline the newly proposed unauthorised disclosure offences contained in the New Zealand Intelligence and Security Bill 2016.

Crimes Act 1961 section 78 – Espionage

A.247 There are two types of espionage offence under section 78, both have maximum sentences of 14 years' imprisonment.

[365] Public Interest Disclosure Act 2013, s 41(1).

[366] Public Interest Disclosure Act 2013, s 6(1) item 3.

A.248 First, section 78(a) makes it an offence for a person who owes allegiance to the Sovereign in right of New Zealand, regardless of whether or not they are in New Zealand, to communicate information or deliver any object to a country or organisation outside of New Zealand or to a person acting on a country or organisation's behalf.

A.249 Secondly, section 78(b) makes it an offence to collect or record any information; copy any document; obtain any object; make any sketch, plan, model or note; take any photograph; record any sound or image; or deliver any object to any person.

A.250 Significantly, for both offences the communication or delivery, or intended communication or delivery, must be likely to prejudice the security or defence of New Zealand.[367]

A.251 For both offences, the person must do so with the intention of prejudicing the security or defence of New Zealand, and, in the case of section 78(b), with the further intention of communicating or delivering the information or object to a country or organisation outside of New Zealand or to a person acting on a country or organisation's behalf.

A.252 It is a question of law, in the case of unauthorised disclosure offences, whether the communication or delivery, or intended communication or intended delivery, was, or would have been, at the time of the alleged offence, likely to have prejudiced the security or defence of New Zealand.[368]

Crimes Act 1961 section 78A – Wrongful communication, retention, or copying of official information

A.253 The New Zealand Official Secrets Act 1951 was repealed by the New Zealand Official Information Act 1982. The offences were retained and brought within the scope of the Crimes Act 1961, where they remain in place today. A prosecution under either section 78 or 78A(1) may only be brought with the consent of the Attorney General.[369]

A.254 Similarly to the offence of espionage, this provision applies to those "who owe allegiance to the Sovereign in right of New Zealand, within or outside New Zealand" and establishes three types of offence:[370]

(1) Section 78A(1)(a) – communicating any official information or delivering any object to any other person. The fault element that must accompany the conduct is knowingly or recklessly communicating or delivering the information/object; with knowledge that he/she is acting without proper authority; and knowing that such communication or delivery is likely to prejudice the security or defence of New Zealand.

[367] Crimes Act 1961, s 78.

[368] Crimes Act 1961, s 78C(1).

[369] Crimes Act 1961, s 78B(1).

[370] Crimes Act 1961, s 78.

(2) Section 78A(1)(b) – retaining or copying any official document which would, by its unauthorised disclosure, be likely to prejudice the security or defence of New Zealand. The fault element requirements are that the person must do the act with the intent to prejudice the security or defence of New Zealand; with knowledge that he/she does not have proper authority to retain or copy the document; and with knowledge that the document relates to the security or defence of New Zealand.

(3) Section 78A(1)(c) – knowingly failing to comply with any direction issued by a lawful authority for the return of an official document which is under his or her possession or control, which would, by its unauthorised disclosure, be likely to prejudice seriously the security or defence of New Zealand. In order to amount to an offence, the person must know the document relates to security or defence of New Zealand.

A.255 The key terms of the offences are broadly defined. For example, "object" includes any information held by a department, organisation, independent contractor engaged by a department or organisation or an unincorporated body that is established to assist or advice any department or Minister.[371] By way of further example, "official information" refers to any information held by a department, Minister of the Crown, organisation, employee of any department or organisation or an independent contractor of any department or Minister.

A.256 Those found guilty of an offence under section 78A are liable to a prison sentence of up to 3 years' imprisonment.[372]

Summary Offences Act 1981 section 20A – Unauthorised disclosure of certain official information

A.257 This provision applies to "every person", not just those who owe an allegiance to the Sovereign of New Zealand (which is the case for the offences under the Crimes Act 1961). Once again, a prosecution under section 20A may only be brought with the consent of the Attorney General.[373]

A.258 It is an offence under section 20A(1) of the Summary Offences Act 1981 knowingly to communicate official information or deliver an object (both as defined in section 78A of Crimes Act) to any other person. Both the knowing communication and delivery versions of the offence require:

(1) that the person must do so knowing he or she does not have proper authority to effect the communication or delivery; and

(2) that the person must know that the communication/delivery is likely to: endanger the safety of any person; prejudice the maintenance of confidential sources of certain classes of information; prejudice the effectiveness of operational plans for the prevention, investigation, or detection of offences or the maintenance of public order; prejudice the safeguarding of life or property in a disaster or emergency; prejudice the

[371] Crimes Act 1961, s 78A(2) .

[372] Crimes Act 1961, s 78A(1).

[373] Summary Offences Act 1981, s 28A(2).

safe custody of offenders or of persons charged with offences; or damage seriously the economy of New Zealand.[374]

A.259 The maximum available sentence is imprisonment for 3 months or a fine not exceeding $2,000.[375]

Security Intelligence Service Act 1969 section 12A – Prohibition on unauthorised disclosure of information

A.260 It is an offence for a current or former officer or employee of the Security and Intelligence Service to disclose or use any information gained by or conveyed to him or her through his or her connection with the Service, unless:

(1) It is in the strict course of his or her official duties; or

(2) It is authorised by the Minister.

A.261 There are two further offences that relate specifically to persons who are authorised to intercept or seize any communication or to undertake electronic tracking in accordance with an intelligence warrant, visual surveillance warrant, or authorisation under section 4ID(1) of the Act. It is a criminal offence for such a person either to:

(1) Disclose the existence of the warrant, or disclose or use any information gained by or conveyed to him when acting pursuant to the warrant, otherwise than as authorised by the warrant or by the Minister or the Director;[376] or

(2) Knowingly to disclose that information outside of the course of his or her duty.[377]

A.262 The maximum sentence for offences under section 12A is imprisonment for a term not exceeding 2 years or a fine not exceeding $2,000.

New Zealand Intelligence and Security Bill 2016

A.263 The New Zealand Intelligence and Security Bill 2016 was placed before the New Zealand Parliament on 15 August 2016. The aim of the Bill is to update the legislative framework and improve the transparency of New Zealand's intelligence and security agencies. The Bill also introduces a number of new offences and terms.

NEW TERMS INTRODUCED BY THE NEW ZEALAND INTELLIGENCE AND SECURITY BILL 2016

A.264 An "employee", in relation to an intelligence and security agency, means a person employed in any capacity in that agency.[378]

[374] Summary Offences Act 1981, s 28A(1)(a) to (f).

[375] Summary Offences Act 1981 s 20A(1).

[376] Security Intelligence Service Act 1969, s 12A(2) [as amended by the New Zealand Security Intelligence Service Amendment Act 2011].

[377] Security Intelligence Service Act 1969, s 12A(3) [as amended by the New Zealand Security Intelligence Service Amendment Act 2014].

A.265 A "foreign organisation" means a Government of any jurisdiction other than New Zealand; an entity controlled by the Government of any jurisdiction other than New Zealand; A body corporate that is incorporated outside New Zealand, or any company within the meaning of the Companies Act 1993 that is, for the purposes of the Companies Act 1993, a subsidiary of any body corporate incorporated outside New Zealand; an unincorporated body of persons that is not a body 50% or more of whose members are New Zealand citizens or permanent residents of New Zealand, and that carries on activities wholly or in part outside New Zealand; and an international organisation.[379]

A.266 To "access" information means to inspect the information; copy the information, or any part of the information; or to obtain a printout of any information.[380]

A.267 "National security" means the protection against—

(1) threats, or potential threats, to New Zealand's status as a free and democratic society from unlawful acts or foreign interference;

(2) imminent threats to the life and safety of New Zealanders overseas;

(3) threats, or potential threats, that may cause serious harm to the safety or quality of life of the New Zealand population;

(4) unlawful acts, or acts of foreign interference, that may cause serious damage to New Zealand's economic security or international relations;

(5) threats, or potential threats, to the integrity of information or infrastructure of critical importance to New Zealand;

(6) threats, or potential threats, that may cause serious harm to the safety of a population of another country as a result of unlawful acts by a New Zealander that are ideologically, religiously, or politically motivated; or

(7) threats, or potential threats, to international security.

A.268 "Sensitive information" is defined by reference to two requirements: that the information is a specific kind of information and that its disclosure would be likely to have a specific result.

(1) The kinds of information that is regarded as sensitive information are as follows:

(a) information that might lead to the identification of, or provide details of sources of information available to, an intelligence and security agency or other assistance or operational methods available to an intelligence and security agency;

[378] The New Zealand Intelligence and Security Bill 2016, part 1, cl 4.

[379] The New Zealand Intelligence and Security Bill 2016, part 1, cl 4.

[380] The New Zealand Intelligence and Security Bill 2016, part 3, cl 36.

(b) information about particular operations that have been undertaken, or are being or are proposed to be undertaken, in carrying out of any of the functions of an intelligence and security agency;

(c) information that has been provided to an intelligence and security agency by another department or agency of the Government of New Zealand and is information that cannot be disclosed by the intelligence and security agency without the consent of the department or agency of the Government of New Zealand by which that information has been provided; and

(d) information that has been provided to an intelligence and security agency by the Government of any other country or by an agency of such a Government and is information that cannot be disclosed by the intelligence and security agency without the consent of the Government or agency by which that information has been provided.

(2) The result that "sensitive information" must be likely to have is to:

(a) prejudice the security or defence of New Zealand or the international relations of the Government of New Zealand;

(b) prejudice the entrusting of information to the Government of New Zealand on a basis of confidence by the Government of any other country or any agency of such a Government or any international organisation;

(c) prejudice the maintenance of the law, including the prevention, investigation, and detection of offences and the right to a fair trial; or

(d) endanger the safety of any person.

NEW OFFENCES INTRODUCED BY THE NEW ZEALAND INTELLIGENCE AND SECURITY BILL 2016

A.269 Clause 206 of the Bill inserts a new disclosure offence into the Crimes Act 1961, section 78AA,[381] which mirrors the "wrongful communication, retention, or copying of official information" offence under section 78A. The new offence, however, differs in several ways:

(1) The new offence criminalises the wrongful communication, retention, or copying of *classified* information, rather than official information under section 78A. Classified information is interpreted wider than official information as:

(a) information that—

(i) is, or was, official information; and

[381] The New Zealand Intelligence and Security Bill 2016, part 8, cl 207.

(ii) is classified under the New Zealand Government Security Classification System as being accessible only to persons who have a national security clearance

(b) foreign government information that is—

(i) classified in a foreign country; and

(ii) accessible only to persons having a New Zealand Government sponsored national security clearance

(2) The new disclosure offence under section 78AA applies only to a person who holds, or has held, a New Zealand Government-sponsored national security clearance to access classified information; or a person to whom classified information has been disclosed in confidence if the disclosure is authorised, and the person knows that the disclosure is in respect of classified information.

(3) The offence of communicating classified information under 78AA(1) does not require knowledge on behalf of the defendant that such communication or delivery is likely to prejudice the security or defence of New Zealand.

(4) The offence of retaining or copying classified information under 78AA(2) does not require the defendant to intend to prejudice the security or defence of New Zealand; know that such classified information relates to the security or defence of New Zealand; or impose a damage requirement that such classified information would, by its unauthorised disclosure, be likely to prejudice the security or defence of New Zealand.

(5) The offence of failing to comply with any directions for the return of an official document under section 78(3) does not require either knowledge that the official document relates to the security or defence of New Zealand or impose a damage requirement that such classified information would, by its unauthorised disclosure, be likely to prejudice the security or defence of New Zealand.

A.270 Two new disclosure offences are also contained in clauses 85 and 86 relating to the disclosure of information obtained whilst carrying out an “authorised activity”. An authorised activity means an activity that is authorised by an intelligence warrant; an authorisation given by the director-general of an intelligence and security agency under section 77; or a removal warrant. Clause 85 criminalises the unlawful disclosure of any information obtained from carrying out an authorised activity. Clause 86 extends the reach of clause 85 by criminalising the unlawful disclosure of any knowledge acquired which derives from information obtained from carrying out an authorised activity. These clauses together can therefore be said together to criminalise the unlawful disclosure of any information obtained directly from, and incidentally to, the carrying out of an authorised activity. Both offences carry a maximum sentence of a fine not exceeding $10,000.

Mechanisms that allow for the protected disclosure of official information

A.271 This section will examine the Protected Disclosure Act 2000, the Inspector-General of Intelligence and Security Act 1996 and discuss proposed changes to the mechanisms contained in the New Zealand Intelligence and Security Bill 2016.

Protected Disclosure Act 2000

A.272 The purpose of the Protected Disclosure Act 2000 is to promote the public interest by facilitating the disclosure and investigation of matters of serious wrongdoing in authorities, and protecting the employees that make such disclosures.[382] The Act requires public organisations to ensure internal procedures are in place for receiving and dealing with information about serious wrongdoing within or by that organisation.

A.273 The Act applies broadly to an "employee of an organisation".[383]An organisation is in turn defined widely as "a body of persons, whether corporate or unincorporate, and whether in the public sector or in the private sector".[384] An employee includes a former employee, a secondee to, and contractor or volunteer with the organisation; as well as a member of the armed forces.[385]

A.274 The kinds of disclosures that will be protected under the Act are set out in section 6:

> Section 6(1) An employee of an organisation may disclose information in accordance with this Act if—
>
> (a) the information is about serious wrongdoing in or by that organisation; and
>
> (b) the employee believes on reasonable grounds that the information is true or likely to be true; and
>
> (c) the employee wishes to disclose the information so that the serious wrongdoing can be investigated; and
>
> (d) the employee wishes the disclosure to be protected.

A.275 For the purposes of the Act, serious wrongdoing includes the following (regardless of whether they occurred before or after the Act was introduced):

(1) unlawful, corrupt, or irregular use of funds or resources of a public sector organisation;

(2) conduct that constitutes a serious risk to public health, public safety or the environment;

[382] Protected Disclosure Act 2000, s 5.

[383] Protected Disclosure Act 2000, s 6(1).

[384] Protected Disclosure Act 2000, s 3(1).

[385] Protected Disclosure Act 2000, s 3(1).

(3) conduct that constitutes a serious risk to the maintenance of law, including the prevention, investigation, and detection of offences and the right to a fair trial;

(4) conduct that amounts to an offence;

(5) conduct by a public official that is oppressive, improperly discriminatory; or

(6) grossly negligent, or that constitutes gross mismanagement.[386]

A.276 The employee must disclose information in the manner provided by internal procedures established by and published in the organisation for receiving and dealing with information about serious wrongdoing.[387] The Act does not protect disclosures where the person makes allegations they know to be false or otherwise acts in bad faith.[388]

A.277 Notwithstanding the requirements set out in section 6(1), an employee may enjoy the protections of the Protected Disclosure Act 2000 in two circumstances. First, if the employee of an organisation believes on reasonable grounds that the information he or she discloses is about serious wrongdoing in or by that organisation but the belief is mistaken, then the information must be treated as complying with subsection (1)(a).[389] Second, when the employee makes a technical failure to comply with the disclosure procedures in sections 7 and 10 or does not expressly refer to the name of this Act when the disclosure is made and, aside from this, the employee has substantially complied with the requirement in section 6.[390]

A.278 A person who makes a protected disclosure of information, or refers a protected disclosure of information to an appropriate authority, is not liable to any civil or criminal proceedings, or a disciplinary proceeding, for having made or referred the disclosure.[391]

A.279 This applies despite any prohibition or restriction on the disclosure of information under any other law,[392] such as the Crimes Act 1961 or Summary Offences Act 1981 mentioned above. The agency or Ombudsman that receives the disclosure of information must "use his or her best endeavors" not to disclose information that might expose the identity of the discloser.[393]

[386] Protected Disclosure Act 2000, s 3(1).

[387] Protected Disclosure Act 2000, s 7(1).

[388] Protected Disclosure Act 2000, s 20.

[389] Protected Disclosure Act 2000, s 6(3).

[390] Protected Disclosure Act 2000, s 6A(1)(a) to (b).

[391] Protected Disclosure Act 2000, s 18(1).

[392] Protected Disclosure Act 2000, s 18(2).

[393] Protected Disclosure Act 2000, s 19(1).

A.280 The Act seeks to institutionalise the practice of public interest disclosures within the public sector through section 11, which requires that every public sector organisation must have in operation appropriate internal procedures for receiving and dealing with information about serious wrongdoing in or by that organisation. These procedures must comply with the principles of natural justice; identify the persons in the organisation to whom a disclosure may be made; and make reference to the statutory forms disclosure may take; and provide information about the internal procedures and how to use them.[394]

A.281 Additionally, the Office of the Ombudsman plays a significant role in providing information and guidance for employees making, or considering to make, a disclosure.[395] Indeed, if an employee notifies the Ombudsman about their intention to make disclosure, the Ombudsman must offer this information and guidance.[396] The Ombudsman may also request an organisation to provide a copy of its internal procedures and their operation.[397]

A.282 There are four outlets for an employee of an organisation to make a disclosure, dependent on the particular circumstances.

(1) Disclosure in accordance with internal procedures, as established and published by the organisation.[398]

(2) Disclosure to the head of an organisation. A disclosure can only be made this way in two circumstances. First, if the organisation has no internal procedures established and published for receiving and dealing with information about serious wrongdoing. Second, if the employee thinks the person to whom the wrongdoing should be reported is involved, or associated with a person involved in the wrongdoing.[399]

(3) Disclosure to an appropriate authority, but only if the person making the disclosure believes, on reasonable grounds, that the head of the organisation may be involved in the serious wrongdoing; it is required by reason of the urgency of the matter to which the disclosure relates, or some other exceptional circumstances; or there has been no action or recommended action on the matter to which the discloser relates within 20 working days after the disclosure was made.[400]

[394] Protected Disclosure Act 2000, s 8(1)(a) to (c).

[395] Protected Disclosure Act 2000, s 6B(1)

[396] Protected Disclosure Act 2000, s 6B(2)(a) to (e).

[397] Protected Disclosure Act 2000, s 6C(1).

[398] Protected Disclosure Act 2000, s 7.

[399] Protected Disclosure Act 2000, s 8.

[400] Protected Disclosure Act 2000, s 9.

(4) Disclosure to a Minister or the Ombudsman, provided that the employee making the disclosure has already made substantially the same disclosure in accordance with the three procedures just mentioned above; he or she continues to reasonably believe the information disclosed is true/likely to be true; he or she reasonably believes the person/authority to whom the disclosure was made: has decided not to investigate the matter, decided to investigate but not made progress with the investigation after a reasonable period of time or has investigated the matter but not taken any action in respect of the matter.[401]

A.283 In addition to overseeing the arrangements that organisations have put in place pursuant to the Act, the Ombudsman also enjoys powers of investigation and can escalate disclosure to an appropriate authority or Minister.[402] Particularly noteworthy is the Ombudsman's power to take over an investigation of a disclosure of information by a public sector organisation, or investigate the disclosure in conjunction with it.[403]

A.284 There are separate disclosure procedures for security and intelligence agencies and certain other organisations. In such cases, the only appropriate authority to whom information may be disclosed, and advice sought from, is the Inspector-General of Intelligence and Security.[404] No disclosure may be made to an Ombudsman or Minister of the Crown other than the minister responsible for the relevant intelligence and security agency or the Prime Minister.[405]

A.285 The Protected Disclosure Act 2000 also requires that the internal procedures of certain public organisations (including the Department of the Prime Minister and Cabinet and the Ministry of Defence) must restrict disclosure of information to the Ombudsman only, with the exception that disclosures may be made to the Prime Minister or Minister responsible for intelligence in the case of disclosures relating to intelligence and security matters.[406]

[401] Protected Disclosure Act 2000, s 10.

[402] Protected Disclosure Act 2000, s 15.

[403] Protected Disclosure Act 2000, s 15A.

[404] Protected Disclosure Act 2000, s 12(b).

[405] Protected Disclosure Act 2000 s 12(d).

[406] Protected Disclosure Act 2000, s 13(h)(ii). Section 13(h)(i) sets out a similar rule which applies in relation to foreign affairs and trade.

Inspector-General of Intelligence and Security Act 1996

A.286 The Inspector-General of Intelligence and Security has a statutory role, under the Intelligence and Security Act 1996, to inquire into any complaint by an employee or former employee of an intelligence and security agency (as well as any other New Zealand person) that the person may have been adversely affected by any act, omission, practice, policy or procedure of an intelligence and security agency.[407] However, this is limited to the extent that the complaint will only be investigated by the Inspector-General if the employee/former employee has established that all internal remedies have been exhausted (unless the employee/former employee and chief executive of the relevant agency agree in writing).[408]

A.287 The Inspector-General enjoys extensive powers of inquiry, these include:

(1) requiring any person to give information relating to any matter to which an inquiry relates to furnish such information;

(2) to produce such documents or things in the possession or under the control of that person;[409] and

(3) the power to summon and examine on oath any person who in the opinion of the Inspector-General is able to give any information relating to any matter to which an inquiry relates.[410]

A.288 Where an inquiry is conducted by the Inspector-General following a complaint, the Inspector-General will prepare a written report containing his or her conclusions[411] and may make such recommendations for the redress of the complaint as he or she thinks fit (including compensation).[412] As well as forwarding the report to the Minister and Chief Executive of the relevant intelligence and security agency, the Inspector-General will advise the complainant of his or her conclusions[413] and must make the report publicly available online.[414]

[407] Intelligence and Security Act 1996, s 11(1)(b)(ii).

[408] Intelligence and Security Act 1996, s 11(5).

[409] Intelligence and Security Act 1996, s 23(1).

[410] Intelligence and Security Act 1996, s 23(2)

[411] Intelligence and Security Act 1996, s 25(1).

[412] Intelligence and Security Act 1996, s 11(6).

[413] Intelligence and Security Act 1996, s 25(2). The information contained in the report provided to the complainant is limited to the extent its terms must not prejudice the security or defence of New Zealand or the international relations of the Government of New Zealand.

[414] Intelligence and Security Act 1996, s 5A(1).

A.289 The Intelligence and Security Act 1996 states an employee of an intelligence or security agency who brings any matter to the attention of the Inspector-General will not be subjected to any penalty or discriminatory treatment of any kind in relation to his or her employment because of having brought a matter to the attention of the Inspector-General (unless it is determined that the employee did so in bad faith).[415] For the purposes of the Act, the term "any matter" could presumably include disclosures of wrongdoing by the intelligence and security agencies. Whilst the Act does prohibit retaliatory responses, it does not make such action a criminal offence or provide any kind of sanction or punishment.

New Zealand Intelligence and Security Bill 2016

A.290 As discussed above, the aim of the New Zealand Intelligence and Security Bill 2016 is to update the legislative framework and improve the transparency of New Zealand's intelligence and security agencies. The Bill repeals the New Zealand Security Intelligence Service Act 1969, the Intelligence and Security Committee Act 1996, the Inspector-General of Intelligence and Security Act 1996, and the Government Communications Security Bureau Act 2003 and makes consequential amendments to many other enactments.[416]

A.291 The Bill, whilst repealing the Inspector-General of Intelligence and Security Act 1996, sets out the functions, duties and powers of the Inspector-General in substantially the same terms as under the previous Act. Clause 121 sets out, however, that an inquiry undertaken by the Inspector-General into any matter relating to an intelligence and security agency's compliance with the law, or into the propriety of an intelligence and security agency's actions, will now be able to be requested by the Intelligence and Security Committee. Clause 123 re-enacts section 18 of the Inspector-General of Intelligence and Security Act 1996 and affords protection to employees of intelligence and security agencies who, in good faith, bring any matter to the attention of the Inspector-General. Such employees may not suffer penalty or discrimination from their employer as a consequence of bringing matters to the attention of the Inspector-General.

A.292 Clause 267 of the Bill also extends the requirement of intelligence and security agencies to produce rules about to whom a protected disclosure may be made by extending the duty to any other organisation in the public sector that holds or has access to classified information or information relating to the activities of an intelligence and security agency.

[415] Intelligence and Security Act 1996, s 18.

[416] The New Zealand Intelligence and Security Bill 2016, part 8, cl 200-280.

SOUTH AFRICA

A.293 This section will first outline the unauthorised disclosure and espionage offences contained in the Protection of Information Act 1982. The section will then examine the Protected Disclosures Act 2000, which provides for the protected disclosure of official information.

Criminal offences for unauthorised disclosures

A.294 The Official Secrets Act 1911 was the law in South Africa until 1954, when it was repealed and replaced by the South African Official Secrets Act 1956. This was then superseded by the Protection of Information Act 1982, which remains in force today as the primary official secrets legislation.[417] Described by the Nelson Mandela Foundation as a "tenacious survivor of the old order",[418] the 1982 Act has been subject to extensive, and deeply contested, legislative reform efforts since 2008. It should be noted that there is no statutory crime of espionage and only a limited number of espionage related common-law offences.[419] The focus of this section is the Protection of Information Act 1982.

Protection of Information Act 84 of 1982 section 2 – Prohibition of certain acts in relation to prohibited places

A.295 Any person who approaches, inspects, passes over, is in the neighbourhood of, or enters any prohibited place for any purpose prejudicial to the security or interests of the Republic, shall be guilty of an offence and liable on conviction to imprisonment for a period not exceeding 20 years.

A.296 For the purposes of the Act "any prohibited place" includes any work of defence belonging to or occupied or used by or on behalf of the Government, any place where armaments are stored or document relating to them.[420] Under section 14 the President may declare any place or area to be a prohibited place where:

(1) He or she is satisfied that information relating to that place or area could be of use to a foreign state or a hostile organisation; or

(2) Any association of persons, movement or institution outside of South Africa to be a hostile organisation if he/she is satisfied that they incite, instigate, command, aid, advise, encourage or procure any person in South Africa or elsewhere to commit an act of violence in South Africa for any purpose prejudicial to the security or interests of South Africa.

[417] For a detailed discussion of the historical context and application of these statutes see S Africa, *Well Kept Secrets: The Right of Access to Information and the South African Intelligence Services* (2009) ch 2.

[418] I Currie and J Klaaren, "Evaluating the Information Bills: A Briefing Paper on the Protection of Informational Bill" (The Nelson Mandela Foundation, 17 June 2011).

[419] For further discussion, see I Currie and J Klaaren, "Evaluating the Information Bills: A Briefing Paper on the Protection of Informational Bill" (The Nelson Mandela Foundation, 17 June 2011), p 10.

[420] Protection of Information Act 1982, s 1.

Protection of Information Act 84 of 1982 section 3 – Prohibition of the obtaining and disclosure of certain information

A.297 In order for a trial or preparatory examination based on the offence in section 3, and every other section of the Act, to commence, the authority concerned must receive written authority from the Attorney General.[421]

A.298 There are two offences within section 3 that apply to any person. The first, under section 3(a), concerns any secret official code or password or any document, model, article or information used, kept, made or obtained in any prohibited place. It is an offence to obtain or receive such information. The second, under section 3(b), concerns any document, model, article or information relating to: any prohibited place or anything in any prohibited place; the defence of the Republic, any military matter, any security matter or the prevention or combating of terrorism; or any other matter or article, and which he knows or reasonably should know may directly or indirectly be of use to any foreign State or any hostile organisation and which, for considerations of the security or the other interests of the Republic, should not be disclosed to any foreign State or to any hostile organisation.

A.299 The phrase "hostile organization" means either any organisation declared by or under any Act of Parliament to be an unlawful organisation or, any association of persons or any movement or institution declared under section 14 of the Protection of Information Act 1982 to be a hostile organisation.

A.300 Section 14 provides that the President may declare any place or area to be a prohibited place if he is satisfied that information with respect to that place or area, or the loss, damage, disruption or immobilisation thereof could be of use to a foreign State or a hostile organisation. Similarly, section 14 provides that the President may declare any association of persons, movement or institution outside the Republic to be a hostile organisation if he is satisfied that that association of persons, movement or institution incites, instigates, commands, aids, advises, encourages or procures any person in the Republic or elsewhere to commit in the Republic an act of violence for any purpose prejudicial to the security or interests of the Republic, and may in like manner at any time repeal or amend any such proclamation.

A.301 The fault element for both offences is that the prohibited conduct must be done for the purposes of disclosure to any foreign State or to any agent, or to any employee or inhabitant of, or any organisation, party, institution, body or movement in, any foreign State, or to any hostile organisation or to any office-bearer, officer, member or active supporter of any hostile organisation. According to the Act, it will be presumed that a defendant acted for the purposes of disclosure to a foreign state or hostile organisation, where the defendant has communicated, or attempted to communicate with an agent in South Africa, or where the defendant is, or is reasonably suspected of being, an agent themselves.[422]

[421] Protection of Information Act 1982, s 12.

[422] Protection of Information Act 1982, s 8(1). The criteria for "communicating with an agent" include visiting an address associated with an agent or addressing communications to such an address: Protection of Information Act 1982, s 8(2)(a) to (b).

A.302 A person found guilty under section 3 is liable to up to 20 years' imprisonment.

Protection of Information Act 84 of 1982 section 4(1) – Prohibition of the disclosure of certain information

A.303 There are several offences, based around different types of information and conduct, which are collected within section 4(1).

A.304 The section applies to any person who has in his or her possession or under his or her control or at his or her disposal either of two types of information:

(1) any official secret or password or

(2) any document, model, article or information which: the person knows or should know relates to a prohibited place; has been made, obtained or received in contravention of the Protection of Information Act; has been entrusted to the person by any government person; has been obtained or accessed by virtue of the person's position as an office/former office holder under the government or contractor of the government/contractor in a prohibited place and knows or should reasonably know the information is secret; or person A has obtained in any manner information from person B, where person B themselves breached the last two conditions mentioned (entrusted in confidence or obtained by virtue or persons position). It is an offence for such a person to:

(a) disclose the information to any person other than a person to whom he/she is authorised to disclose it or to whom it may lawfully be disclosed or to whom, in the interests of South Africa, it is his duty to disclose it;

(b) publish or use the information in any manner or for any purpose which is prejudicial to the security or interests of South Africa;

(c) retain the information or fail to comply with any lawful directions to return or dispose of the information; or

(d) neglect to take proper care of the information.

A.306 Those found guilty under section 4 are liable to imprisonment for up to 10 years and/or a fine of up to R10,000. Significantly, though, if the prosecution can prove that the defendant published or disclosed either types of information referred to in section 4 for the purpose of it being disclosed to a foreign state or hostile organisation, the defendant may be sentenced to up to 20 years' imprisonment.

Protection of Information Act 84 of 1982 section 4(2) – Prohibition of the disclosure of certain information

A.307 It is an offence for any person to receive any official code or password or any document, model, article or information, who knows or has reasonable grounds to believe that information being disclosed to them is in contravention of the Protection of Information Act. To avoid liability under this section, the defendant must prove that the disclosure was against their wishes.

A.308 Mirroring section 4(1), those found guilty under section 4(2) are liable to imprisonment for up to10 years and/or a fine of up to R10,000.

Protection of Information Act 84 of 1982 section 5(2) – Prohibition of certain acts prejudicial to security or interests of Republic

A.309 There are several lesser offences contained in section 5(2) that overlap to some degree with those just mentioned but apply to any person. It is an offence to do any of the following.

(1) Retain any official document for purposes prejudicial to the security or interests of South Africa.

(2) Allow any other person to have possession of any official document issued for his or her use alone.

(3) Possess any official document or secret official code or password issued for the use of another person, without lawful authority or excuse.

(4) Neglect or fail to hand over any official document to the person or authority by whom or for whose use it was issued or to a member of the South African Police Service.

(5) Manufacture or sell, or have in one's possession for sale, any die, seal or stamp without lawful authority or excuse.

A.310 Those found guilty under section 5(2) are liable to imprisonment for up to 5 years and/or a fine of up to R5,000.

Mechanisms that allow for the protected disclosure of official information – Protected Disclosure Act 26 of 2000

A.311 The purpose of the Protected Disclosure Act 2000 is to create procedures through which private and public sector employees can disclose information regarding unlawful or irregular conduct by their employers or other employees, and be protected for having disclosed such information.

A.312 The Act applies to an "employee", which means:

(1) any person, excluding an independent contractor, who works for another person or for the state, and who receives, or is entitled to receive remuneration; or

(2) any other person who in any manner assists in carrying on or conducting the business of an employer.

A.313 The status of volunteer workers is unclear under the Protected Disclosure Act 2000. The requirement that an employee must receive, or be entitled to receive, remuneration appears to rule them out, however, voluntary work could be seen as assisting in carrying out or conducting business.[423]

A.314 Section 1 of the Protected Disclosure Act 2000 defines a disclosure as:

[423] Protected Disclosures Act 2000, s 1.

Any disclosure of information regarding any conduct of an employer, or an employee of that employer, made by any employee who has reason to believe that the information concerned shows or tends to show one or more of the following:

(a) that a criminal offence has been committed, is being committed or is likely to be committed;

(b) that a person has failed, is failing or is likely to fail to comply with any legal obligation to which that person is subject;

(c) that a miscarriage of justice has occurred, is occurring or is likely to occur;

(d) that the health or safety of an individual has been, is being or is likely to be endangered;

(e) that the environment has been, is being or is likely to be damaged;

(f) unfair discrimination as contemplated in the Promotion of Equality and Prevention of Unfair Discrimination Act 2000; or

(g) that any matter referred to in paragraphs (a) to (f) has been, is being or is likely to be deliberately concealed.

A.315 To be a protected disclosure under the Protected Disclosure Act 2000, the disclosure must be made to one of the following person/bodies and made in accordance with the respective rules that apply to that person/body:

(1) A legal adviser (section 5).

(2) An employer (section 6, notably: good faith requirement, following any internal procedure prescribed or authorised by the employer). It should be noted that under section 10(4) of the Protected Disclosure Act 2000, the Minister for the Administration of Justice must issue practical guidelines which explain the provisions of this Act and all procedures which are available in terms of any law to employees who wish to report or otherwise remedy an impropriety.

(3) A member of Cabinet or of the Executive Council of a province (section 7).

(4) A person or body in accordance with section 8 (includes Public Protector (the South African equivalent of a Whistleblower Protection Authority) and Auditor General, the impropriety at issue must:

(a) Fall within any description of matters which are dealt with by the person or body concerned; and

(b) Be substantially true.

(5) Any other person or body (section 9).

A.316 It is worth reflecting more closely on the rules set out in section 9, due to the more stringent conditions:

(1) Such a disclosure will not be protected where the employee commits an offence by making that disclosure or where a legal adviser discloses information they received from a person in the course of obtaining legal advice in accordance with section 5.[424]

(2) A disclosure must be made in good faith by an employee. That is, the employee must reasonably believe the information or allegation being disclosed is true and the discloser is not being made by the employee for "for purposes of personal gain, excluding any reward payable in terms of any law".[425]

(3) At least one or more of the following conditions must be present *and* in all the circumstances of the case, it is deemed by the court to reasonable to make the disclosure:[426]

(a) The employee who makes the disclosure has reason to believe that he or she will be subjected to an occupational detriment if they make a disclosure to their employer in accordance with section 6.

(b) In a case where no person/body is prescribed for the purposes of section 8 in relation to the relevant impropriety, the employee making the disclosure has reason to believe that it is likely that evidence relating to the impropriety will be concealed or destroyed if they make the disclosure to their employer.

(c) The employee making the disclosure has previously made a disclosure of substantially the same information to his or her employer or persona or agency per section 8 and no action was taken after a reasonable period of time.

(d) The impropriety is of an exceptionally serious nature.[427]

A.317 The Protected Disclosures Act 2000 prohibits certain contractual conditions and occupational conduct as the primary means of protection for those who make disclosures under its conditions. It relies on pre-existing employment law remedies where adverse conditions or conduct takes place.

[424] Protected Disclosures Act 2000, s 1.

[425] Protected Disclosures Act 2000, s 9(1)(a) to (b).

[426] Protected Disclosures Act 2000, s 9(1). In determining whether it is reasonable in all the circumstances, the court must consider the factors set out in Protected Disclosures Act 2000, s 9(3)(a) to (g).

[427] Protected Disclosures Act 2000, s 9(2)(a) to (d).

A.318 The Act makes a contract of employment or other agreement between an employer and an employee void if the contract purports to exclude any provision of the Protected Disclosure Act 2000 or precludes or discourages the employee from making a protected disclosure.[428]

A.319 The Act prohibits "occupational detriment" in the working environment resulting from an employee's disclosure.[429] Conduct that amounts to "occupational detriment" is being:

(1) subjected to any disciplinary action;

(2) dismissed, suspended, demoted, harassed or intimidated;

(3) transferred against his or her will;

(4) refused transfer or promotion;

(5) subjected to a term or condition of employment or retirement which is altered or kept altered to his or her disadvantage;

(6) refused a reference, or being provided with an adverse reference, from his or her employer;

(7) denied appointment to any employment, profession or office;

(8) threatened with any of the actions referred to paragraphs (a) to (g) above; or

(9) being otherwise adversely affected in respect of his or her employment, profession or office, including employment opportunities and work security.[430]

A.320 Anyone subject to "occupational detriment" under section 3 of the Protected Disclosure Act 2000 may approach any court having jurisdiction for appropriate relief or pursue any other processed allowed by law.[431] Any dismissal in breach of section 3 is deemed to be an automatically unfair dismissal as contemplated in section 187 of the Labour Relations Act 1995 and any other occupational detriment in breach of section 3 is deemed to be an unfair labour practice under the Labour Relations Act 1995.[432]

[428] Protected Disclosures Act 2000 s 2(3).

[429] Protected Disclosures Act 2000, s 3.

[430] Protected Disclosures Act 2000, s 1.

[431] Protected Disclosures Act 2000, s 4(1)(a) to (b).

[432] Protected Disclosures Act 2000, s 4(2)(a) to (b).

APPENDIX B
GOVERNMENT DEPARTMENTS, ORGANISATIONS AND INDIVIDUALS CONSULTED

B.1 This appendix lists the government departments, organisations and individuals with whom we have consulted during our initial consultation and whose views have informed our provisional conclusions and consultation questions.

Government Departments

(1) Attorney General's Office.

(2) Cabinet Office.

(3) Defence and Security Media Advisory Committee.

(4) Department for Work and Pensions.

(5) Foreign and Commonwealth Office.

(6) Government Legal Department.

(7) Her Majesty's Revenue and Customs.

(8) Her Majesty's Treasury.

(9) Home Office.

(10) Ministry of Defence.

(11) Ministry of Justice.

Agencies, police and prosecuting authorities

(1) Army Legal Service.

(2) Crown Prosecution Service.

(3) Government Communication Headquarters (GCHQ).

(4) Information Commissioner's Office.

(5) Metropolitan Police Service.

(6) Security Service (MI5).

(7) Police Service of Northern Ireland.

(8) Secret Intelligence Service (MI6).

(9) Service Prosecution Authority.

(10) Treasury Counsel.

Individuals and members of the judiciary

(1) David Anderson QC.

(2) Dean Armstrong QC.

(3) Alex Bailin QC.

(4) Joel Bennathan QC.

(5) Dan Hyde.

(6) The Rt Hon Dominic Grieve QC MP.

(7) The Rt Hon Sir Stephen Irwin.

(8) Julian Knowles QC.

(9) Gavin Millar QC.

(10) Tim Moloney QC.

(11) The Hon Sir Andrew Nicol.

(12) Tim Owen QC.

(13) Matthew Ryder QC.

(14) Chris Saad.

(15) Dr Ashley Savage.

(16) The Hon Sir Keir Starmer QC MP.

(17) Aidan Wills.

(18) The Judges of the Central Criminal Court.

Organisations

(1) Guardian Media.

(2) News Media UK.

(3) News Corporation.

(4) Liberty.

(5) Open Rights Group.

(6) Public Concern at Work.

APPENDIX C
WIDER UNAUTHORISED DISCLOSURE OFFENCES

INTRODUCTION

C.1 This appendix sets out the wider unauthorised disclosure offences that we have uncovered during our research. We do not, however, consider this to be a definitive list, but it does serve to demonstrate the quantity of disclosure offences that presently exist.

(1) Section 11 of the Atomic Energy Act 1946.

(2) Section 13 of the Atomic Energy Act 1946.

(3) Section 56 of the Coal Industry Nationalisation Act 1946.

(4) Section 5 of the Industrial Organisation and Development Act 1947.

(5) Section 9 of the Statistics of Trade Act 1947.

(6) Section 22 of the Prevention of Damage by Pests Act 1949.

(7) Section 47 of the Agricultural Marketing Act 1958.

(8) Section 12 of the Rivers (Prevention of Pollution) Act 1961.

(9) Section 46 of the Harbours Act 1964.

(10) Schedule 6 of the Gas Act 1965.

(11) Section 118 of the Medicines Act 1968.

(12) Section 14 of the Sea Fish Industry Act 1970.

(13) Schedule 4 of the Counter-Inflation Act 1973.

(14) Section 9 of the Employment Agencies Act 1973.

(15) Section 33 of the Health and Safety at Work etc. Act 1974.

(16) Section 9 of the Rehabilitation of Offenders Act 1974.

(17) Section 9A of the Rehabilitation of Offenders Act 1974.

(18) Section 6 of the Supply Powers Act 1975.

(19) Regulation 9 of the Carriage of Goods (Prohibition of Discrimination) Regulations 1977/276.

(20) Section 4 of the Agricultural Statistics Act 1979.

(21) Section 292 of the Highways Act 1980.

(22) Section 12 of the Fisheries Act 1981.

(23) Regulation 9 of the Milk Marketing Boards (Special Conditions) Regulations 1981/322.[1]

(24) Section 54 of the Public Passenger Vehicles Act 1981.

(25) Section 23 of the Civil Aviation Act 1982.

(26) Section 6 of the Industrial Training Act 1982.

(27) Section 33 of the Iron and Steel Act 1982.

(28) Section 10 of the Merchant Shipping (Liner Conferences) Act 1982.

(29) Section 96 of the Building Act 1984.

(30) Section 43 of the Road Traffic Regulation Act 1984.

(31) Section 101 of the Telecommunications Act 1984.

(32) Section 449 of the Companies Act 1985.

(33) Section 74 of the Airports Act 1986.

(34) Section 86 Companies Act 1989.

(35) Section 98 of the Electricity Act 1989.

(36) Section 182 of the Finance Act 1989.

(37) Section 174 of the Water Act 1989.

(38) Section 197 of the Broadcasting Act 1990.

(39) Section 41 of the Human Fertilisation and Embryology Act 1990.

(40) Section 196C of the Town and Country Planning Act 1990.

(41) Section 325 of the Town and Country Planning Act 1990.

(42) Schedule 15 of the Town and Country Planning Act 1990.

(43) Section 50 of the Child Support Act 1991.

(44) Section 91 of the Criminal Justice Act 1991.

(45) Section 206 of the Water Industry Act 1991.

(46) Section 204 of the Water Resources Act 1991.

(47) Section 205(5) of the Water Resources Act 1991.

[1] The regulation was revoked with regards to England by Environment and Rural Affairs (Miscellaneous Revocations) Regulations 2015/639, reg 3(a) (April 1, 2015).

(48) Section 205(6) of the Water Resources Act 1991.

(49) Section 123 of the Social Security Administration Act 1992.

(50) Schedule 7 of the Cardiff Bay Barrage Act 1993.

(51) Section 4C of the National Lottery Act 1993.

(52) Section 145 of the Railways Act 1993.

(53) Section 14 of the Criminal Justice and Public Order Act 1994.

(54) Section 23 of the Criminal Appeal Act 1995.

(55) Section 35 of the Goods Vehicles (Licensing of Operators) Act 1995.

(56) Section 3 of the Shipping and Trading Interests (Protection) Act 1995.

(57) Section 32 of the Chemical Weapons Act 1996.

(58) Regulation 23 of the Airports (Groundhandling) Regulations 1997/2389.

(59) Schedule 7 of the Bank of England Act 1998.

(60) Section 55 of the Data Protection Act 1998.

(61) Section 59 of the Data Protection Act 1998.

(62) Section 19 of the Landmines Act 1998.

(63) Regulation 29 of the Working Time Regulations 1998/1833.

(64) Section 158 of the Immigration and Asylum Act 1999.

(65) Section 6 of the Nuclear Safeguards Act 2000.

(66) Section 19 of the Regulation of Investigatory Powers Act 2000.

(67) Section 3 of the Television Licences (Disclosure of Information) Act 2000.

(68) Section 143 of the Transport Act 2000.

(69) Schedule 9 of the Transport Act 2000.

(70) Schedule 10 of the Transport Act 2000.

(71) Section 105 of the Utilities Act 2000.

(72) Section 79 of the Anti-terrorism, Crime and Security Act 2001.

(73) Section 80 of the Anti-terrorism, Crime and Security Act 2001.

(74) Section 19 of the Private Security Industry Act 2001.

(75) Section 245 of the Enterprise Act 2002.

(76) Section 393 of the Communications Act 2003.

(77) Regulation 25 of the Nuclear Industries Security Regulations 2003/403.

(78) Section 15C of the Companies (Audit, Investigations and Community Enterprise) Act 2004.

(79) Section 2 of the Pensions Act 2004.

(80) Section 197 of the Pensions Act 2004.

(81) Section 54 of the Public Audit (Wales) Act 2004.

(82) Regulation 19 of the Access to Information (Post-Commencement Adoptions) (Wales) Regulations 2005/2689.

(83) Section 19 of the Commissioners for Revenue and Customs Act 2005.

(84) Regulation 21 of the Disclosure of Adoption Information (Post-Commencement Adoptions) Regulations 2005/888.

(85) Section 109 of the Education Act 2005.

(86) Section 111 of the Education Act 2005.

(87) Regulation 17 of the Road Transport (Working Time) Regulations 2005/639.

(88) Section 1 of the Armed Forces Act 2006.

(89) Section 17 of the Armed Forces Act 2006.

(90) Section 13B of the Childcare Act 2006.

(91) Section 458 of the Companies Act 2006.

(92) Section 460 of the Companies Act 2006.

(93) Section 949 if the Companies Act 2006.

(94) Section 1224B of the Companies Act 2006.

(95) Section 6 of the Equality Act 2006.

(96) Section 205 of the National Health Service Act 2006.

(97) Schedule 10 of the National Health Service Act 2006.

(98) Schedule 22 of the National Health Service Act 2006.

(99) Section 111 of the Wireless Telegraphy Act 2006.

(100) Section 39 of the Statistics and Registration Service Act 2007.

(101) Section 102 of the Tribunals, Courts and Enforcement Act 2007.[2]

(102) Section 42 of the UK Borders Act 2007.

(103) Regulation 11 of the Cross-border Railway Services (Working Time) Regulations 2008/1660.

(104) Section 76 of the Health and Social Care Act 2008.

(105) Section 18 of the Borders, Citizenship and Immigration Act 2009.

(106) Section 23 of the Cluster Munitions (Prohibitions) Act 2010.

(107) Section 56 of the Postal Services Act 2011.

(108) Regulation 39 of the Trade in Animals and Related Products Regulations 2011/1197.

(109) Regulation 39 of the Trade in Animals and Related Products (Wales) Regulations 2011/2379.

(110) Schedule 6 of the Civil Aviation Act 2012.

(111) Regulation 3 of the Customs Disclosure of Information and Miscellaneous Amendments Regulations 2012/1848.

(112) Regulation 334 of the Human Medicines Regulations 2012/1916.

(113) Section 33 of the Legal Aid, Sentencing and Punishment of Offenders Act 2012.

(114) Section 34 of the Legal Aid, Sentencing and Punishment of Offenders Act 2012.

(115) Section 129 of the Welfare Reform Act 2012.

(116) Regulation 22 of the Construction Products Regulations 2013/1387.

(117) Schedule 7 paragraph 10(1) of the Crime and Courts Act 2013.

(118) Schedule 7 paragraph 10(2) of the Crime and Courts Act 2013.

(119) Schedule 9 of the Energy Act 2013.

(120) Schedule 5 of the Defence Reform Act 2014.

(121) Schedule 11 of the Local Audit and Accountability Act 2014.

(122) Section 8 of the Mesothelioma Act 2014.

(123) Schedule 10 paragraph 15 of the Criminal Justice and Courts Act 2015.

(124) Schedule 10 paragraph 25 of the Criminal Justice and Courts Act 2015.

[2] The offence is not yet in force.

APPENDIX D
THE OFFICIAL SECRETS ACTS 1911, 1920 AND 1989

D.1 This Appendix provides relevant extracts from the text of the of following legislation:

(1) The Official Secrets Act 1911 (as amended by the Official Secrets Act 1920).

(2) The Official Secrets Act 1920 (as amended by the Official Secrets Act 1939).

(3) The Official Secrets Act 1989.

Official Secrets Act 1911

An Act to re-enact the Official Secrets Act 1889 with Amendments.

[22nd August 1911]

1. Penalties for spying.

(1) If any person for any purpose prejudicial to the safety or interests of the State—

(a) approaches, inspects, passes over or is in the neighbourhood of, or enters any prohibited place within the meaning of this Act; or

(b) makes any sketch, plan, model, or note which is calculated to be or might be or is intended to be directly or indirectly useful to an enemy; or

(c) obtains, collects, records, or publishes, or communicates to any other person any secret official code word, or pass word, or any sketch, plan, model, article, or note, or other document or information which is calculated to be or might be or is intended to be directly or indirectly useful to an enemy;

he shall be guilty of felony.

(2) On a prosecution under this section, it shall not be necessary to show that the accused person was guilty of any particular act tending to show a purpose prejudicial to the safety or interests of the State, and, notwithstanding that no such act is proved against him, he may be convicted if, from the circumstances of the case, or his conduct, or his known character as proved, it appears that his purpose was a purpose prejudicial to the safety or interests of the State; and if any sketch, plan, model, article, note, document, or information relating to or used in any prohibited place within the meaning of this Act, or anything in such a place or any secret official code word or pass word, is made, obtained, collected, recorded, published, or communicated by any person other than a person acting under lawful authority, it shall be deemed to have been made, obtained, collected, recorded, published or communicated for a purpose prejudicial to the safety or interests of the State unless the contrary is proved.

3. Definition of prohibited place.

(1) For the purposes of this Act, the expression “prohibited place” means—

(a) any work of defence, arsenal, naval or air force establishment or station, factory, dockyard, mine, minefield, camp, ship, or aircraft belonging to or occupied by or on behalf of His Majesty, or any telegraph, telephone, wireless or signal station, or office so belonging or occupied, and any place belonging to or occupied by or on behalf of His Majesty and used for the purpose of building, repairing, making, or storing any munitions of war, or any sketches, plans, models or documents relating thereto, or for the purpose of getting any metals, oil, or minerals of use in time of war;

(b) any place not belonging to His Majesty where any munitions of war, or any sketches, models, plans or documents relating thereto, are being made, repaired, gotten, or stored under contract with, or with any person on behalf of, His Majesty, or otherwise on behalf of His Majesty; and

(c) any place belonging to or used for the purposes of His Majesty which is for the time being declared by order of a Secretary of State to be a prohibited place for the purposes of this section on the ground that information with respect thereto, or damage thereto, would by useful to an enemy; and

(d) any railway, road, way, or channel, or other means of communication by land or water (including any works or structures being part thereof or connected therewith), or any place used for gas, water, or electricity works or other works for purposes of a public character, or any place where any munitions of war, or any sketches, models, plans or documents relating thereto, are being made, repaired, or stored otherwise than on behalf of His Majesty, which is for the time being declared by order of a Secretary of State to be a prohibited place for the purposes of this section, on the ground that information with respect thereto, or the destruction or obstruction thereof, or interference therewith, would be useful to an enemy.

6. Power to arrest.

Any person who is found committing an offence under this Act, whether that offence is a felony or not, or who is reasonably suspected of having committed, or having attempted to commit, or being about to commit, such an offence, may be apprehended and detained in the same manner as a person who is found committing a felony.

7. Penalty for harbouring spies.

If any person knowingly harbours any person whom he knows, or has reasonable grounds for supposing, to be a person who is about to commit or who has committed an offence under this Act, or knowingly permits to meet or assemble in any premises in his occupation or under his control any such persons, or if any person having harboured any such person, or permitted to meet or assemble in any premises in his occupation or under his control any such persons, wilfully omits or refuses to disclose to a superintendent of police any information which it is in his power to give in relation to any such person he shall be guilty of a misdemeanour.

8. Restriction on prosecution.

A prosecution for an offence under this Act shall not be instituted except by or with the consent of the Attorney-General.

9. Search Warrants.

(1) If a justice of the peace is satisfied by information on oath that there is reasonable ground for suspecting that an offence under this Act has been or is about to be committed, he may grant a search warrant authorising any constable to enter at any time any premises or place named in the warrant, if necessary, by force, and to search the premises or place and every person found therein, and to seize any sketch, plan, model, article, note, or document, or anything of a like nature or anything which is evidence of an offence under this Act having been or being about to be committed, which he may find on the premises or place or on any such person, and with regard to or in connexion with which he has reasonable ground for suspecting that an offence under this Act has been or is about to be committed.

(2) Where it appears to a superintendent of police that the case is one of great emergency and that in the interest of the State immediate action is necessary, he may by a written order under his hand give to any constable the like authority as may be given by the warrant of a justice under this section.

10. Extent of Act and place of trial of offence.

(1) This Act shall apply to all acts which are offences under this Act when committed in any part of His Majesty's dominions, or when committed by British Officers or subjects elsewhere.

(2) An offence under this Act, if alleged to have been committed out of the United Kingdom, may be inquired of, heard, and determined, in any competent British court in the place where the offence was committed, or in England.

(3) An offence under this Act shall not be tried by any court of general session, nor by the sheriff court in Scotland, nor by any court out of the United Kingdom which has not jurisdiction to try crimes which involve the greatest punishment allowed by law.

11. Saving for laws of British possessions.

If by any law made before or after the passing of this Act by the legislature of any British possession provisions are made which appear to His Majesty to be of the like effect as those contained in this Act, His Majesty may, by Order in Council, suspend the operation within that British possession of this Act, or of any part thereof, so long as that law continues in force there, and no longer.

Provided that the suspension of this Act, or of any part thereof, in any British possession shall not extend to the holder of an office under His Majesty who is not appointed to that office by the Government of that possession.

12. Interpretation.

In this Act, unless the context otherwise requires,—

Any reference to a place belonging to His Majesty includes a place belonging to any department of the Government of the United Kingdom or of any British possessions, whether the place is or is not actually vested in His Majesty;

The expression “Attorney-General” means the Attorney-General for England; and as respects Scotland, means the Lord Advocate; and as respects Ireland, means the Advocate General for Northern Ireland; and, if the prosecution is instituted in any court out of the United Kingdom, means the person who in that court is Attorney-General, or exercises the like functions as the Attorney-General in England;

Expressions referring to communicating include any communicating, whether in whole or in part, and whether the sketch, plan, model, article, note, document, or information itself or the substance, effect, or description thereof only be communicated; expressions referring to obtaining or retaining any sketch, plan, model, article, note, or document, include the copying or causing to be copied the whole or any part of any sketch, plan, model, article, note, or document; and expressions referring to the communication of any sketch, plan, model, article, note or document include the transfer or transmission of the sketch, plan, model, article, note or document;

The expression “document” includes part of a document;

The expression “model” includes design, pattern, and specimen;

The expression “sketch” includes any photograph or other mode of representing any place or thing;

The expression “munitions of war” includes the whole or any part of any ship, submarine, aircraft, tank or similar engine, arms and ammunition, torpedo, or mine, intended or adapted for use in war, and any other article, material, or device, whether actual or proposed, intended for such use;

The expression “superintendent of police” includes any police officer of a like or superior rank and any person upon whom the powers of a superintendent of police are for the purposes of this Act conferred by a Secretary of State;

The expression “office under His Majesty” includes any office or employment in or under any department of the Government of the United Kingdom, or of any British possession;

The expression “offence under this Act” includes any act, commission, or other thing which is punishable under this Act.

13. Short title and repeal.

(1) This Act may be cited as the Official Secrets Act 1911.

Official Secrets Act 1920

An Act to amend the Official Secrets Act 1911.

[23rd December 1920]

1. Unauthorised use of uniforms; falsification of reports, forgery, personation, and false documents.

(1) If any person for the purpose of gaining admission, or of assisting any other person to gain admission, to a prohibited place, within the meaning of the Official Secrets Act 1911 (hereinafter referred to as "the principal Act"), or for any other purpose prejudicial to the safety or interests of the State within the meaning of the said Act—

(a) uses or wears, without lawful authority, any naval, military, air-force, police, or other official uniform, or any uniform so nearly resembling the same as to be calculated to deceive, or falsely represents himself to be a person who is or has been entitled to use or wear any such uniform; or

(b) orally, or in writing in any declaration or application, or in any document signed by him or on his behalf, knowingly makes or connives at the making of any false statement or any omission; or

(c) tampers with any passport or any naval, military, air-force, police, or official pass, permit, certificate, licence, or other document of a similar character (hereinafter in this section referred to as an official document), or has in his possession any forged, altered, or irregular official document; or

(d) personates, or falsely represents himself to be a person holding, or in the employment of a person holding office under His Majesty, or to be or not to be a person to whom an official document or secret official code word or pass word has been duly issued or communicated, or with intent to obtain an official document, secret official code word or pass word, whether for himself or any other person, knowingly makes any false statement; or

(e) uses, or has in his possession or under his control, without the authority of the Government Department or the authority concerned, any die, seal, or stamp of or belonging to, or used, made or provided by any Government Department, or by any diplomatic, naval, military, or air-force authority appointed by or acting under the authority of His Majesty, or any die, seal or stamp so nearly resembling any such die, seal or stamp as to be calculated to deceive, or counterfeits any such die, seal or stamp, or uses, or has in his possession, or under his control, any such counterfeited die, seal or stamp;

he shall be guilty of a misdemeanour.

(2) If any person—

(a) retains for any purpose prejudicial to the safety or interests of the State any official document, whether or not completed or issued for use, when he has no right to retain it, or when it is contrary to his duty to retain it, or fails to comply with any directions issued by any Government Department or any person authorised by such department with regard to the return or disposal thereof; or

(b) allows any other person to have possession of any official document issued for his use alone, or communicates any secret official code word or pass word so issued, or, without lawful authority or excuse, has in his possession any official document or secret official code word or pass word issued for the use of some person other than himself, or on obtaining possession of any official document by finding or otherwise, neglects or fails to restore it to the person or authority by whom or for whose use it was issued, or to a police constable; or

(c) without lawful authority or excuse, manufactures or sells, or has in his possession for sale any such die, seal or stamp as aforesaid;

he shall be guilty of a misdemeanour.

(3) In the case of any prosecution under this section involving the proof of a purpose prejudicial to the safety or interests of the State, subsection (2) of section one of the principal Act shall apply in like manner as it applies to prosecutions under that section.

2. Communications with foreign agents to be evidence of commission of certain offences.

(1) In any proceedings against a person for an offence under section one of the principal Act, the fact that he has been in communication with, or attempted to communicate with, a foreign agent, whether within or without the United Kingdom, shall be evidence that he has, for a purpose prejudicial to the safety or interests of the State, obtained or attempted to obtain information which is calculated to be or might be or is intended to be directly or indirectly useful to an enemy.

(2) For the purpose of this section, but without prejudice to the generality of the foregoing provision—

(a) A person shall, unless he proves the contrary, be deemed to have been in communication with a foreign agent if—

(i) He has, either within or without the United Kingdom, visited the address of a foreign agent or consorted or associated with a foreign agent; or

(ii) Either, within or without the United Kingdom, the name or address of, or any other information regarding a foreign agent has been found in his possession, or has been supplied by him to any other person, or has been obtained by him from any other person:

(b) The expression “foreign agent” includes any person who is or has been or is reasonably suspected of being or having been employed by a foreign power either directly or indirectly for the purpose of committing an act, either within or without the United Kingdom, prejudicial to the safety or interests of the State, or who has or is reasonably suspected of having, either within or without the United Kingdom, committed, or attempted to commit, such an act in the interests of a foreign power:

(c) Any address, whether within or without the United Kingdom, reasonably suspected of being an address used for the receipt of communications intended for a foreign agent, or any address at which a foreign agent resides, or to which he resorts for the purpose of giving or receiving communications, or at which he carries on any business, shall be deemed to be the address of a foreign agent, and communications addressed to such an address to be communications with a foreign agent.

3. Interfering with officers of the police or members of His Majesty's forces.

No person in the vicinity of any prohibited place shall obstruct, knowingly mislead or otherwise interfere with or impede, the chief officer or a superintendent or other officer of police, or any member of His Majesty's forces engaged on guard, sentry, patrol, or other similar duty in relation to the prohibited place, and, if any person acts in contravention of, or fails to comply with, this provision, he shall be guilty of a misdemeanour.

6. Duty of giving information as to commission of offences.

(1) Where a chief officer of police is satisfied that there is reasonable ground for suspecting that an offence under section one of the principal Act has been committed and for believing that any person is able to furnish information as to the offence or suspected offence, he may apply to a Secretary of State for permission to exercise the powers conferred by this subsection and, if such permission is granted, he may authorise a superintendent of police, or any police officer not below the rank of inspector, to require the person believed to be able to furnish information to give any information in his power relating to the offence or suspected offence, and, if so required and on tender of his reasonable expenses, to attend at such reasonable time and place as may be specified by the superintendent or other officer; and if a person required in pursuance of such an authorisation to give information, or to attend as aforesaid, fails to comply with any such requirement or knowingly gives false information, he shall be guilty of a misdemeanour.

(2) Where a chief officer of police has reasonable grounds to believe that the case is one of great emergency and that in the interest of the State immediate action is necessary, he may exercise the powers conferred by the last foregoing subsection without applying for or being granted the permission of a Secretary of State, but if he does so shall forthwith report the circumstances to the Secretary of State.

(3) References in this section to a chief officer of police shall be construed as including references to any officer of police expressly authorised by a chief officer of police to act on his behalf for the purposes of this section when by reason of illness, absence, or other cause he is unable to do so.

7. Attempts, incitements, &c.

Any person who attempts to commit any offence under the principal Act or this Act, or solicits or incites or endeavours to persuade another person to commit an offence, or aids or abets and does any act preparatory to the commission of an offence under the principal Act or this Act, shall be guilty of a felony or a misdemeanour or a summary offence according as the offence in question is a felony, a misdemeanour or a summary offence, and on conviction shall be liable to the same punishment, and to be proceeded against in the same manner, as if he had committed the offence.

8. Provisions as to trial and punishment of offences.

(1) Any person who is guilty of a felony under the principal Act or this Act shall be liable to penal servitude for a term of not less than three years and not exceeding fourteen years.

(2) Any person who is guilty of a misdemeanour under the principal Act or this Act shall be liable on conviction on indictment to imprisonment, for a term not exceeding two years, or, on conviction under the Summary Jurisdiction Acts, to imprisonment, for a term not exceeding three months or to a fine not exceeding the prescribed sum, or both such imprisonment and fine:

Provided that no misdemeanour under the principal Act or this Act shall be dealt with summarily except with the consent of the Attorney General.

(3) For the purposes of the trial of a person for an offence under the principal Act or this Act, the offence shall be deemed to have been committed either at the place in which the same actually was committed, or at any place in the United Kingdom in which the offender may be found.

(4) In addition and without prejudice to any powers which a court may possess to order the exclusion of the public from any proceedings if, in the course of proceedings before a court against any person for an offence under the principal Act or this Act or the proceedings on appeal, or in the course of the trial of a person for felony or misdemeanour under the principal Act or this Act, application is made by the prosecution, on the ground that the publication of any evidence to be given or of any statement to be made in the course of the proceedings would be prejudicial to the national safety, that all or any portion of the public shall be excluded during any part of the hearing, the court may make an order to that effect, but the passing of sentence shall in any case take place in public.

(5) Where the person guilty of an offence under the principal Act or this Act is a company or corporation, every director and officer of the company or corporation shall be guilty of the like offence unless he proves that the act or omission constituting the offence took place without his knowledge or consent.

11. Short title, construction, and repeal.

(1) This Act may be cited as the Official Secrets Act 1920, and shall be construed as one with the principal Act, and the principal Act and this Act may be cited together as the Official Secrets Acts 1911 and 1920:

Provided that—

(b) nothing in the principal Act shall be construed as preventing an offence under this Act which is to be tried summarily being tried in Scotland by the Sheriff.

(1A) For the purposes of this Act as it extends to Northern Ireland, the expression "chief officer of police" means a superintendent or chief superintendent of the Royal Ulster Constabulary.

Official Secrets Act 1989

An Act to replace section 2 of the Official Secrets Act 1911 by provisions protecting more limited classes of official information.

[11th May 1989]

1. Security and intelligence.

(1) A person who is or has been—

(a) a member of the security and intelligence services; or

(b) a person notified that he is subject to the provisions of this subsection,

is guilty of an offence if without lawful authority he discloses any information, document or other article relating to security or intelligence which is or has been in his possession by virtue of his position as a member of any of those services or in the course of his work while the notification is or was in force.

(2) The reference in subsection (1) above to disclosing information relating to security or intelligence includes a reference to making any statement which purports to be a disclosure of such information or is intended to be taken by those to whom it is addressed as being such a disclosure.

(3) A person who is or has been a Crown servant or government contractor is guilty of an offence if without lawful authority he makes a damaging disclosure of any information, document or other article relating to security or intelligence which is or has been in his possession by virtue of his position as such but otherwise than as mentioned in subsection (1) above.

(4) For the purposes of subsection (3) above a disclosure is damaging if—

(a) it causes damage to the work of, or of any part of, the security and intelligence services; or

(b) it is of information or a document or other article which is such that its unauthorised disclosure would be likely to cause such damage or which falls within a class or description of information, documents or articles the unauthorised disclosure of which would be likely to have that effect.

(5) It is a defence for a person charged with an offence under this section to prove that at the time of the alleged offence he did not know, and had no reasonable cause to believe, that the information, document or article in question related to security or intelligence or, in the case of an offence under subsection (3), that the disclosure would be damaging within the meaning of that subsection.

(6) Notification that a person is subject to subsection (1) above shall be effected by a notice in writing served on him by a Minister of the Crown; and such a notice may be served if, in the Minister's opinion, the work undertaken by the person in question is or includes work connected with the security and intelligence services and its nature is such that the interests of national security require that he should be subject to the provisions of that subsection.

(7) Subject to subsection (8) below, a notification for the purposes of subsection (1) above shall be in force for the period of five years beginning with the day on which it is served but may be renewed by further notices under subsection (6) above for periods of five years at a time.

(8) A notification for the purposes of subsection (1) above may at any time be revoked by a further notice in writing served by the Minister on the person concerned; and the Minister shall serve such a further notice as soon as, in his opinion, the work undertaken by that person ceases to be such as is mentioned in subsection (6) above.

(9) In this section “security or intelligence” means the work of, or in support of, the security and intelligence services or any part of them, and references to information relating to security or intelligence include references to information held or transmitted by those services or by persons in support of, or of any part of, them.

2. Defence.

(1) A person who is or has been a Crown servant or government contractor is guilty of an offence if without lawful authority he makes a damaging disclosure of any information, document or other article relating to defence which is or has been in his possession by virtue of his position as such.

(2) For the purposes of subsection (1) above a disclosure is damaging if—

(a) it damages the capability of, or of any part of, the armed forces of the Crown to carry out their tasks or leads to loss of life or injury to members of those forces or serious damage to the equipment or installations of those forces; or

(b) otherwise than as mentioned in paragraph (a) above, it endangers the interests of the United Kingdom abroad, seriously obstructs the promotion or protection by the United Kingdom of those interests or endangers the safety of British citizens abroad; or

(c) it is of information or of a document or article which is such that its unauthorised disclosure would be likely to have any of those effects.

(3) It is a defence for a person charged with an offence under this section to prove that at the time of the alleged offence he did not know, and had no reasonable cause to believe, that the information, document or article in question related to defence or that its disclosure would be damaging within the meaning of subsection (1) above.

(4) In this section “defence” means —

(a) the size, shape, organisation, logistics, order of battle, deployment, operations, state of readiness and training of the armed forces of the Crown;

(b) the weapons, stores or other equipment of those forces and the invention, development, production and operation of such equipment and research relating to it;

(c) defence policy and strategy and military planning and intelligence;

(d) plans and measures for the maintenance of essential supplies and services that are or would be needed in time of war.

3. International relations.

(1) A person who is or has been a Crown servant or government contractor is guilty of an offence if without lawful authority he makes a damaging disclosure of—

(a) any information, document or other article relating to international relations; or

(b) any confidential information, document or other article which was obtained from a State other than the United Kingdom or an international organisation,

being information or a document or article which is or has been in his possession by virtue of his position as a Crown servant or government contractor.

(2) For the purposes of subsection (1) above a disclosure is damaging if—

(a) it endangers the interests of the United Kingdom abroad, seriously obstructs the promotion or protection by the United Kingdom of those interests or endangers the safety of British citizens abroad; or

(b) it is of information or of a document or article which is such that its unauthorised disclosure would be likely to have any of those effects.

(3) In the case of information or a document or article within subsection (1)(b) above—

(a) the fact that it is confidential, or

(b) its nature or contents,

may be sufficient to establish for the purposes of subsection (2)(b) above that the information, document or article is such that its unauthorised disclosure would be likely to have any of the effects there mentioned.

(4) It is a defence for a person charged with an offence under this section to prove that at the time of the alleged offence he did not know, and had no reasonable cause to believe, that the information, document or article in question was such as is mentioned in subsection (1) above or that its disclosure would be damaging within the meaning of that subsection.

(5) In this section "international relations" means the relations between States, between international organisations or between one or more States and one or more such organisations and includes any matter relating to a State other than the United Kingdom or to an international organisation which is capable of affecting the relations of the United Kingdom with another State or with an international organisation.

(6) For the purposes of this section any information, document or article obtained from a State or organisation is confidential at any time while the terms on which it was obtained require it to be held in confidence or while the circumstances in which it was obtained make it reasonable for the State or organisation to expect that it would be so held.

4. Crime and special investigation powers.

(1) A person who is or has been a Crown servant or government contractor is guilty of an offence if without lawful authority he discloses any information, document or other article to which this section applies and which is or has been in his possession by virtue of his position as such.

(2) This section applies to any information, document or other article—

(a) the disclosure of which—

(i) results in the commission of an offence; or

(ii) facilitates an escape from legal custody or the doing of any other act prejudicial to the safekeeping of persons in legal custody; or

(iii) impedes the prevention or detection of offences or the apprehension or prosecution of suspected offenders; or

(b) which is such that its unauthorised disclosure would be likely to have any of those effects.

(3) This section also applies to—

(a) any information obtained by reason of the interception of any communication in obedience to a warrant issued under section 2 of the Interception of Communications Act 1985 or under the authority of an interception warrant under section 5 of the Regulation of Investigatory Powers Act 2000, any information relating to the obtaining of information by reason of any such interception and any document or other article which is or has been used or held for use in, or has been obtained by reason of, any such interception; and

(b) any information obtained by reason of action authorised by a warrant issued under section 3 of the Security Service Act 1989 or under section 5 of the Intelligence Services Act 1994 or by an authorisation given under section 7 of that Act, any information relating to the obtaining of information by reason of any such action and any document or other article which is or has been used or held for use in, or has been obtained by reason of, any such action.

(4) It is a defence for a person charged with an offence under this section in respect of a disclosure falling within subsection (2)(a) above to prove that at the time of the alleged offence he did not know, and had no reasonable cause to believe, that the disclosure would have any of the effects there mentioned.

(5) It is a defence for a person charged with an offence under this section in respect of any other disclosure to prove that at the time of the alleged offence he did not know, and had no reasonable cause to believe, that the information, document or article in question was information or a document or article to which this section applies.

(6) In this section “legal custody” includes detention in pursuance of any enactment or any instrument made under an enactment.

5. Information resulting from unauthorised disclosures or entrusted in confidence.

(1) Subsection (2) below applies where—

(a) any information, document or other article protected against disclosure by the foregoing provisions of this Act has come into a person's possession as a result of having been—

(i) disclosed (whether to him or another) by a Crown servant or government contractor without lawful authority; or

(ii) entrusted to him by a Crown servant or government contractor on terms requiring it to be held in confidence or in circumstances in which the Crown servant or government contractor could reasonably expect that it would be so held; or

(iii) disclosed (whether to him or another) without lawful authority by a person to whom it was entrusted as mentioned in sub-paragraph (ii) above; and

(b) the disclosure without lawful authority of the information, document or article by the person into whose possession it has come is not an offence under any of those provisions.

(2) Subject to subsections (3) and (4) below, the person into whose possession the information, document or article has come is guilty of an offence if he discloses it without lawful authority knowing, or having reasonable cause to believe, that it is protected against disclosure by the foregoing provisions of this Act and that it has come into his possession as mentioned in subsection (1) above.

(3) In the case of information or a document or article protected against disclosure by sections 1 to 3 above, a person does not commit an offence under subsection (2) above unless—

(a) the disclosure by him is damaging; and

(b) he makes it knowing, or having reasonable cause to believe, that it would be damaging;

and the question whether a disclosure is damaging shall be determined for the purposes of this subsection as it would be in relation to a disclosure of that information, document or article by a Crown servant in contravention of section 1(3), 2(1) or 3(1) above.

(4) A person does not commit an offence under subsection (2) above in respect of information or a document or other article which has come into his possession as a result of having been disclosed—

(a) as mentioned in subsection (1)(a)(i) above by a government contractor; or

(b) as mentioned in subsection (1)(a)(iii) above,

unless that disclosure was by a British citizen or took place in the United Kingdom, in any of the Channel Islands or in the Isle of Man or a colony.

(5) For the purposes of this section information or a document or article is protected against disclosure by the foregoing provisions of this Act if—

(a) it relates to security or intelligence, defence or international relations within the meaning of section 1, 2 or 3 above or is such as is mentioned in section 3(1)(b) above; or

(b) it is information or a document or article to which section 4 above applies;

and information or a document or article is protected against disclosure by sections 1 to 3 above if it falls within paragraph (a) above.

(6) A person is guilty of an offence if without lawful authority he discloses any information, document or other article which he knows, or has reasonable cause to believe, to have come into his possession as a result of a contravention of section 1 of the Official Secrets Act 1911.

6. Information entrusted in confidence to other States or international organisations.

(1) This section applies where—

(a) any information, document or other article which—

(i) relates to security or intelligence, defence or international relations; and

(ii) has been communicated in confidence by or on behalf of the United Kingdom to another State or to an international organisation,

has come into a person's possession as a result of having been disclosed (whether to him or another) without the authority of that State or organisation or, in the case of an organisation, of a member of it; and

(b) the disclosure without lawful authority of the information, document or article by the person into whose possession it has come is not an offence under any of the foregoing provisions of this Act.

(2) Subject to subsection (3) below, the person into whose possession the information, document or article has come is guilty of an offence if he makes a damaging disclosure of it knowing, or having reasonable cause to believe, that it is such as is mentioned in subsection (1) above, that it has come into his possession as there mentioned and that its disclosure would be damaging.

(3) A person does not commit an offence under subsection (2) above if the information, document or article is disclosed by him with lawful authority or has previously been made available to the public with the authority of the State or organisation concerned or, in the case of an organisation, of a member of it.

(4) For the purposes of this section “security or intelligence”, “defence” and “international relations” have the same meaning as in section 1, 2 and 3 above and the question whether a disclosure is damaging shall be determined as it would be in relation to a disclosure of the information, document or article in question by a Crown servant in contravention of section 1(3), 2(1) and 3(1) above.

(5) For the purposes of this section information or a document or article is communicated in confidence if it is communicated on terms requiring it to be held in confidence or in circumstances in which the person communicating it could reasonably expect that it would be so held.

7. Authorised disclosures.

(1) For the purposes of this Act a disclosure by—

(a) a Crown servant; or

(b) a person, not being a Crown servant or government contractor, in whose case a notification for the purposes of section 1(1) above is in force,

is made with lawful authority if, and only if, it is made in accordance with his official duty.

(2) For the purposes of this Act a disclosure by a government contractor is made with lawful authority if, and only if, it is made—

(a) in accordance with an official authorisation; or

(b) for the purposes of the functions by virtue of which he is a government contractor and without contravening an official restriction.

(3) For the purposes of this Act a disclosure made by any other person is made with lawful authority if, and only if, it is made—

(a) to a Crown servant for the purposes of his functions as such; or

(b) in accordance with an official authorisation.

(4) It is a defence for a person charged with an offence under any of the foregoing provisions of this Act to prove that at the time of the alleged offence he believed that he had lawful authority to make the disclosure in question and had no reasonable cause to believe otherwise.

(5) In this section "official authorisation" and "official restriction" mean, subject to subsection (6) below, an authorisation or restriction duly given or imposed by a Crown servant or government contractor or by or on behalf of a prescribed body or a body of a prescribed class.

(6) In relation to section 6 above "official authorisation" includes an authorisation duly given by or on behalf of the State or organisation concerned or, in the case of an organisation, a member of it.

8. Safeguarding of information.

(1) Where a Crown servant or government contractor, by virtue of his position as such, has in his possession or under his control any document or other article which it would be an offence under any of the foregoing provisions of this Act for him to disclose without lawful authority he is guilty of an offence if—

(a) being a Crown servant, he retains the document or article contrary to his official duty; or

(b) being a government contractor, he fails to comply with an official direction for the return or disposal of the document or article,

or if he fails to take such care to prevent the unauthorised disclosure of the document or article as a person in his position may reasonably be expected to take.

(2) It is a defence for a Crown servant charged with an offence under subsection (1)(a) above to prove that at the time of the alleged offence he believed that he was acting in accordance with his official duty and had no reasonable cause to believe otherwise.

(3) In subsections (1) and (2) above references to a Crown servant include any person, not being a Crown servant or government contractor, in whose case a notification for the purposes of section 1(1) above is in force.

(4) Where a person has in his possession or under his control any document or other article which it would be an offence under section 5 above for him to disclose without lawful authority, he is guilty of an offence if—

(a) he fails to comply with an official direction for its return or disposal; or

(b) where he obtained it from a Crown servant or government contractor on terms requiring it to be held in confidence or in circumstances in which that servant or contractor could reasonably expect that it would be so held, he fails to take such care to prevent its unauthorised disclosure as a person in his position may reasonably be expected to take.

(5) Where a person has in his possession or under his control any document or other article which it would be an offence under section 6 above for him to disclose without lawful authority, he is guilty of an offence if he fails to comply with an official direction for its return or disposal.

(6) A person is guilty of an offence if he discloses any official information, document or other article which can be used for the purpose of obtaining access to any information, document or other article protected against disclosure by the foregoing provisions of this Act and the circumstances in which it is disclosed are such that it would be reasonable to expect that it might be used for that purposes without authority.

(7) For the purposes of subsection (6) above a person discloses information or a document or article which is official if—

(a) he has or has had it in his possession by virtue of his position as a Crown servant or government contractor; or

(b) he knows or has reasonable cause to believe that a Crown servant or government contractor has or has had it in his possession by virtue of his position as such.

(8) Subsection (5) of section 5 above applies for the purposes of subsection (6) above as it applies for the purposes of that section.

(9) In this section “official direction” means a direction duly given by a Crown servant or government contractor or by or on behalf of a prescribed body or a body of a prescribed class.

9. Prosecutions.

(1) Subject to subsection (2) below, no prosecution for an offence under this Act shall be instituted in England and Wales or in Northern Ireland except by or with the consent of the Attorney General or, as the case may be, the Advocate General for Northern Ireland.

(2) Subsection (1) above does not apply to an offence in respect of any such information, document or article as is mentioned in section 4(2) above but no prosecution for such an offence shall be instituted in England and Wales or in Northern Ireland except by or with the consent of the Director of Public Prosecutions or, as the case may be, the Director of Public Prosecutions for Northern Ireland.

10. Penalties.

(1) A person guilty of an offence under any provision of this Act other than section 8(1), (4) or (5) shall be liable—

(a) on conviction on indictment, to imprisonment for a term not exceeding two years or a fine or both;

(b) on summary conviction, to imprisonment for a term not exceeding six months or a fine not exceeding the statutory maximum or both.

(2) A person guilty of an offence under section 8(1), (4) or (5) above shall be liable on summary conviction to imprisonment for a term not exceeding three months or a fine not exceeding level 5 on the standard scale or both.

11. Arrest, search and trial.

(2) Offences under any provision of this Act other than section 8(1), (4) or (5) and attempts to commit them shall be arrestable offences within the meaning of section 2 of the Criminal Law Act (Northern Ireland) 1967.

(3) Section 9(1) of the Official Secrets Act 1911 (search warrants) shall have effect as if references to offences under that Act included references to offences under any provision of this Act other than section 8(1), (4) or (5); and the following provisions of the Police and Criminal Evidence Act 1984, that is to say—

(a) section 9(2) (which excludes items subject to legal privilege and certain other material from powers of search conferred by previous enactments); and

(b) paragraph 3(b) of Schedule 1 (which prescribes access conditions for the special procedure laid down in that Schedule),

shall apply to section 9(1) of the said Act of 1911 as extended by this subsection as they apply to that section as originally enacted.

(4) Section 8(4) of the Official Secrets Act 1920 (exclusion of public from hearing on grounds of national safety) shall have effect as if references to offences under that Act included references to offences under any provision of this Act other than section 8(1), (4) or (5).

(5) Proceedings for an offence under this Act may be taken in any place in the United Kingdom.

12. "Crown servant" and "government contractor".

(1) In this Act "Crown servant" means —

(a) a Minister of the Crown;

(aa) a member of the Scottish Government or a junior Scottish Minister;

(ab) the First Minister for Wales, a Welsh Minister appointed under section 48 of the Government of Wales Act 2006 , the Counsel General to the Welsh Government or a Deputy Welsh Minister;

(b) a person appointed under section 8 of the Northern Ireland Constitution Act 1973 (the Northern Ireland Executive etc.);

(c) any person employed in the civil service of the Crown, including Her Majesty's Diplomatic Service, Her Majesty's Overseas Civil Service, the civil service of Northern Ireland and the Northern Ireland Court Service;

(d) any member of the naval, military or air forces of the Crown, including any person employed by an association established for the purposes of Part XI of the Reserve Forces Act 1996;

(e) any constable and any other person employed or appointed in or for the purposes of any police force (including the Police Service of Northern Ireland and the Police Service of Northern Ireland Reserve) or an NCA special (within the meaning of Part 1 of the Crime and Courts Act 2013);

(f) any person who is a member or employee of a prescribed body or a body of a prescribed class and either is prescribed for the purposes of this paragraph or belongs to a prescribed class of members or employees of any such body;

(g) any person who is the holder of a prescribed office or who is an employee of such a holder and either is prescribed for the purposes of this paragraph or belongs to a prescribed class of such employees.

(2) In this Act "government contractor" means, subject to subsection (3) below, any person who is not a Crown servant but who provides, or is employed in the provision of, goods or services—

(a) for the purposes of any Minister or person mentioned in paragraph (a), (ab) or (b) of subsection (1) above, of any office-holder in the Scottish Administration, of any of the services, forces or bodies mentioned in that subsection or of the holder of any office prescribed under that subsection;

(b) under an agreement or arrangement certified by the Secretary of State as being one to which the government of a State other than the United Kingdom or an international organisation is a party or which is subordinate to, or made for the purposes of implementing, any such agreement or arrangement.

(3) Where an employee or class of employees of any body, or of any holder of an office, is prescribed by an order made for the purposes of subsection (1) above—

(a) any employee of that body, or of the holder of that office, who is not prescribed or is not within the prescribed class; and

(b) any person who does not provide, or is not employed in the provision of, goods or services for the purposes of the performance of those functions of the body or the holder of the office in connection with which the employee or prescribed class of employees is engaged,

shall not be a government contractor for the purposes of this Act.

(4) In this section "office-holder in the Scottish Administration" has the same meaning as in section 126(7)(a) of the Scotland Act 1998.

(4A) In this section the reference to a police force includes a reference to the Civil Nuclear Constabulary.

(5) This Act shall apply to the following as it applies to persons falling within the definition of Crown servant—

(a) the First Minister and deputy First Minister in Northern Ireland; and

(b) Northern Ireland Ministers and junior Ministers.

13. Other interpretation provisions.

(1) In this Act—

"disclose" and "disclosure", in relation to a document or other article, include parting with possession of it;

"international organisation" means , subject to subsections (2) and (3) below, an organisation of which only States are members and includes a reference to any organ of such an organisation;

"prescribed" means prescribed by an order made by the Secretary of State;

"State" includes the government of a State and any organ of its government and references to a State other than the United Kingdom include references to any territory outside the United Kingdom.

(2) In section 12(2)(b) above the reference to an international organisation includes a reference to any such organisation whether or not one of which only States are members and includes a commercial organisation.

(3) In determining for the purposes of subsection (1) above whether only States are members of an organisation, any member which is itself an organisation of which only States are members, or which is an organ of such an organisation, shall be treated as a State.

14. Orders.

(1) Any power of the Secretary of State under this Act to make orders shall be exercisable by statutory instrument.

(2) No order shall be made by him for the purposes of section 7(5), 8(9) or 12 above unless a draft of it has been laid before, and approved by a resolution of, each House of Parliament.

(3) If, apart from the provisions of this subsection, the draft of an order under any of the provisions mentioned in subsection (2) above would be treated for the purposes of the Standing Orders of either House of Parliament as a hybrid instrument it shall proceed in that House as if it were not such an instrument.

15. Acts done abroad and extent.

(1) Any act—

(a) done by a British citizen or Crown servant; or

(b) done by any person in any of the Channel Islands or the Isle of Man or any colony,

shall, if it would be an offence by that person under any provision of this Act other than section 8(1), (4) or (5) when done by him in the United Kingdom, be an offence under that provision.

(2) This Act extends to Northern Ireland.

(3) Her Majesty may by Order in Council provide that any provision of this Act shall extend, with such exceptions, adaptations and modifications as may be specified in the Order, to any of the Channel Islands or the Isle of Man or any colony.

16. Short title, citation, consequential amendments, repeals, revocation and commencement.

(1) This Act may be cited as the Official Secrets Act 1989.

(2) This Act and the Official Secrets Acts 1911 to 1939 may be cited together as the Official Secrets Acts 1911 to 1989.

(3) Schedule 1 to this Act shall have effect for making amendments consequential on the provisions of this Act.

(4) The enactments and Order mentioned in Schedule 2 to this Act are hereby repealed or revoked to the extent specified in the third column of that Schedule.

(5) Subject to any Order under subsection (3) of section 15 above the repeals in the Official Secrets Act 1911 and the Official Secrets Act 1920 do not extend to any of the territories mentioned in that subsection.

(6) This Act shall come into force on such day as the Secretary of State may by order appoint.