Law Commission
Reforming the law

Protection of Official Data Report

HC 716

Law Com No 395

Law Commission
Reforming the law

Law Com No 395

Protection of Official Data Report

Presented to Parliament pursuant to section 3(2) of the Law Commissions Act 1965

Ordered by the House of Commons to be printed on 1st September 2020

HC 716

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

Any enquiries regarding this publication should be sent to us at pod@lawcommission.gov.uk

ISBN 978-1-5286-2113-7

CCS0820043516 09/20

Printed on paper containing 75% recycled fibre content minimum

Printed in the UK by the APS Group on behalf of the Controller of Her Majesty's Stationery Office

The Law Commission

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

The Law Commissioners are:

The Right Honourable Lord Justice Green, Chairman

Professor Sarah Green

Professor Nick Hopkins

Professor Penney Lewis

Nicholas Paines QC

The Chief Executive of the Law Commission is Phil Golding.

The Law Commission is located at 1st Floor, Tower, 52 Queen Anne's Gate, London SW1H 9AG.

The terms of this report were agreed on 1st July 2020.

The text of this report is available on the Law Commission's website at http://www.lawcom.gov.uk.

Contents

Chapter 1: Introduction

1.1 This Report considers the effectiveness of the criminal law provisions that protect official information and makes recommendations for much needed reform. The provisions are primarily contained in the Official Secrets Acts 1911-1939 and 1989. Some of these provisions relate to those who, being lawfully in possession of official information, disclose it without authorisation (commonly referred to as "leaks"). Other provisions criminalise individuals whose purpose is to gain access to information, potentially by using covert means, sometimes referred to as espionage.

1.2 The scale and potential impact of espionage and of unauthorised disclosures has changed considerably in the 21st century. Developments in technology – such as communications technology, data sharing and storage, and cyber capability generally – mean that the threat of espionage and unauthorised disclosures is of a wholly different order than was the case even twenty years ago.

1.3 The nature of espionage and unauthorised disclosures has also changed significantly. For example, hostile states can conduct cyber-attacks through multiple servers across multiple jurisdictions. Further, the line between states and non-state entities (such as corporations) has become increasingly blurred. These examples, among many others, demonstrate how the changing nature of espionage and unauthorised disclosures frustrates antiquated legislation based on notions of "enemy" states conducting hostile activity within one particular jurisdiction.

1.4 The urgency of this reform was most recently and extensively articulated in the Report on "Russia" of the Intelligence and Security Committee of Parliament, which was laid before Parliament on 21st July 2020. On this point, the Committee concluded:

> it is very clear that the Official Secrets Act regime is not fit for purpose and the longer this goes unrectified, the longer the Intelligence Community's hands are tied.[1]

1.5 Our Report also presents a timely opportunity to assess the compatibility of the current offences with the right to freedom of expression under Article 10 of the European Convention on Human Rights ("ECHR"). We consider the offences in the light of the developments in ECHR case law in the two decades since the matter was last considered by the Appellate Committee of the House of Lords (the predecessor to the UK Supreme Court). We are bound to make recommendations that are compatible with the ECHR and therefore this Report includes an extensive analysis of Article 10 and makes certain recommendations concerning the public interest on the basis of that analysis.

1.6 This Report includes many recommendations for reform, and these are based on independent legal analysis, open consultation and the detailed assessment of evidence. It is, however, a *legal* report approved by the Chairman and the Commissioners, who are lawyers. It deals with highly sensitive matters that are both legally and politically complex. There are questions in the Report to which an

[1] Intelligence and Security Committee of Parliament, *Russia* (HC 632) para 117.

evidence-based legal analysis is able to provide part of the answer; but there are also some important matters that we have considered for which there is no legal answer and which ought properly to be left to the Executive and Parliament as an elected body. We have made clear in the Report where this is the case.

1.7 This Report has benefitted from the insight of a great many consultees, including those in the media, academia and legal services. Similarly, we have also received submissions and evidence from Government and the intelligence community which have enabled us more fully to understand the nature of the risks and threats facing the UK. We are very grateful to all who have contributed to this project, whose insight and evidence has enabled us to reform and refine our analysis over the life of the project.

THE GENESIS OF THIS REPORT

1.8 In July 2015, we were asked by the Rt Hon Matthew Hancock MP, then Minister for the Cabinet Office, to conduct an independent review of the legal framework governing the unauthorised disclosure of government information. In that invitation, the Minister expressed concern that:

> the impact and sensitivity of leaks has increased over time… On a very practical level the Official Secrets Act 1989 does not cover the considerable changes that have occurred in technology, global networks and social media.

1.9 The Minister further wrote:

> Our overall goal is a strengthened commitment to open government and transparency especially through open data, with clearer boundaries, and a safe space for policy discussion. I want to be able to provide those handling sensitive [government] information with the clearest possible expectation of what is required of them, and in instances where things go wrong a clear framework that sets out the consequences.

1.10 Implicit in that statement and a dominant factor throughout the project is that there is a balance to be struck between the need for accountability, on the one hand, and the need for effective protection of sensitive information, on the other.

The terms of reference

1.11 The following terms of reference were agreed with the Cabinet Office in January 2016:

(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.

(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; and

(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.

1.12 Our terms of reference were broad. They included the provisions of the Official Secrets Act 1989 which deal with unauthorised disclosures – leaks. They also extended to a review of the espionage offences in the Official Secrets Acts 1911-1939 and other criminal provisions governing the protection of government information. We were to consider all relevant legislation. We were to research and consult independently on options for an effective and coherent legal response to unauthorised disclosures. We were to consider the relationship between criminal law and any civil remedies. As with all Law Commission reports, any recommendations we made had to be compliant with the ECHR.

The consultation

1.13 We commenced work in February 2016. We met and discussed the issues with stakeholders prior to the publication of "Protection of Official Data – A Consultation Paper" ("the Consultation Paper" or "CP").[2]

1.14 We published the Consultation Paper on 2 February 2017. The Consultation Paper examined the Official Secrets Acts 1911-1939 and 1989, as well as 124 miscellaneous offences of unauthorised disclosure of information held by public bodies, such as the Data Protection Act 1998, the Anti-terrorism, Crime and Security Act 2001, and the Atomic Energy Act 1946. We also considered procedural matters related to prosecutions and investigations under the Official Secrets Acts, examined the compatibility of unauthorised disclosure offences with freedom of expression, and assessed the case for introducing a public interest defence in the Official Secrets Act 1989. Within the Consultation Paper, we included a number of consultation questions and provisional conclusions, to encourage an open, public debate.[3]

---

2 For a list see Appendix to the CP.

3 See further discussion in the CP, para 1.9.

1.15 The Consultation Paper elicited an unprecedented level of response from media organisations, academics, non-governmental organisations, and individual members of the public. Consultees engaged with our proposals, and in some cases had strong and persuasive arguments against some of the provisional positions we adopted.

1.16 There were criticisms, particularly of our treatment of the Official Secrets Act 1989, not least our provisional proposal not to introduce a public interest defence. There was some evident misconception that the proposals in the Consultation Paper were our final view and that they had been arrived at without consultation. In fact, as with all Law Commission projects, the provisional proposals published in the Consultation Paper were just that: provisional and open for consultation. We were in fact very pleased that there was so much engagement with the consultation phase of the project.

1.17 The Consultation Paper attracted a great deal of media attention, some positive or neutral, but a great deal of it negative. There was also a cross party Early Day Motion in Parliament which was critical of the project, and petitions were launched in opposition to the Consultation Paper's proposals. One such petition, submitted by the Open Rights Group, had 23,385 signatories.

1.18 The consultation period was extended by a month and formally closed on 3 May 2017. In view of the level of intense ongoing interest and the volume of responses – over 1,200 in total – subsequent submissions were also accepted. The list of consultees who responded to the consultation is set out in Appendix A.

1.19 As part of the consultation exercise, in March 2017 we conducted a roundtable event hosted by the News Media Association, which was attended by a number of major media organisations.[4] In April 2017, we met with a group of researchers specialising in media law and freedom of expression at the Institute for Advanced Legal Studies, and attended an academic roundtable at the University of Oxford. In June 2017, we held a roundtable event for legal representatives of broadcast and print media groups. In July 2017, Professor David Ormerod QC (then Law Commissioner responsible for Criminal Law) gave a public lecture about the project at the Royal United Services Institute ("RUSI").

1.20 We have also held numerous discussions with various organisations, government departments and professional individuals including journalists, newspaper editors, and members of the judiciary, the Law Society, and the Bar. Organisations we have had discussions with include: The Bar Council and the Criminal Bar Association; Campaign for Freedom of Information; Her Majesty's Inspectorate of Constabulary and Fire & Rescue Services ("HMICFRS"); Index on Censorship / Reporters without Borders; The Law Society; Liberty; Open Rights Group; National Union of Journalists; and Public Concern at Work.

---

4 We are grateful to these organisations for hosting a number of these roundtable events, and to Matrix Chambers for hosting one with legal representatives from media organisations in June 2016, before we published the Consultation Paper.

1.21 As a consultative organisation, we greatly value this detailed and considered feedback from many different sectors. It is a crucial pillar of our work. The responses we received have informed this project and the conclusions contained within this Report.

CLASSIFIED EVIDENCE

1.22 As with all Law Commission reports, much of the evidence on which we rely is provided to us by stakeholders and consultees. This Report is unusual, however, in that some of the evidence relevant to our analysis is highly sensitive – classified as SECRET or TOP SECRET – and spans a range of different subject matters.

1.23 The Law Commission endeavours to operate in the most open and transparent manner possible. The fact that some of the issues that we have considered are so sensitive created a potential problem for us. We were reluctant to approve a final report which was based upon evidence to which we could not refer in the public domain. Were we to cite classified evidence in the Report, it would have to be so heavily redacted as to be of little or no illustrative use. To overcome this, we agreed with the Government and the security services a procedure for dealing with confidential and secret evidence that has enabled us to maintain transparency to the greatest degree possible.

1.24 We agreed that the Government would provide open submissions to us drafted on the basis that everything provided could be referred to in our final report and placed in the public domain. Where the Government wished to illustrate a point with classified evidence (for example, in order to highlight the risks attached to a particular proposal), or where we had requested specific evidence, it would set out hypothetical cases based upon real life experience but would not in those open submissions refer to classified evidence from actual cases. To enable the Commissioners to be confident that the hypothetical examples were a fair reflection of reality, the Commissioner for Criminal Law (Professor Penney Lewis) and the senior lawyer working on the project (Dr Nicholas Hoggard) would be given access to the actual evidence from the intelligence, defence and security services, and they would then form their own, independent, conclusion as to whether the examples in the open submissions could be relied upon.

1.25 This exercise in verification occurred. It included Professor Lewis and Dr Hoggard asking for further details in some cases and being able to question relevant officials from Government and the intelligence community on particular points of concern to them. When the assessment of the classified evidence was complete, Professor Lewis and Dr Hoggard provided a statement to the Commissioners certifying that they were satisfied by the evidence provided that the risks that the hypothetical examples were designed to illustrate are material risks, so that the hypothetical examples could be relied upon by Commissioners. It follows that the only evidence that the other Commissioners took into account when approving the final report is that which is in the public domain. We have included in the final report all of the evidence provided to us in the open submission from Government.

1.26 We are grateful to the government and intelligence community for their cooperation in working with us to enable Commissioners to form their conclusions on the basis of evidence that they could share in this manner with the public.

THE REPORT

1.27 This Report is the culmination of work that began in 2015. It incorporates our background research, analysis of the responses we received to the Consultation Paper, assessment of evidence, and our resulting recommendations. In several respects, the extensive consultation and evidence gathering process has led to conclusions in this Report that we did not have in mind in the early stages of the project.

1.28 As we have explained above, the recommendations we make recognise that the balance to be struck between protecting official data, on the one hand, and government accountability, on the other, involves sensitive political questions. Some of our recommendations deal with matters that are more readily described as matters of law and the recommendations in such cases are often necessarily detailed. In contrast, on some issues our recommendations are drafted in more general terms, recognising that the precise form any new law should take engages matters of politics, which should ultimately be for Parliament to resolve. The most obvious example of this is the recommendation in Chapter 11 for a public interest defence to be introduced into the Official Secrets Act 1989. We make that recommendation on the basis of a legal assessment of Article 10 ECHR (protecting the right to freedom of expression) but do so without prescribing the precise form that such a defence should take: the law only takes the analysis so far.

1.29 This Report is structured in three parts. Part I considers the Official Secrets Acts 1911-1939, and thus is primarily focussed on espionage offences. Part II considers the Official Secrets Act 1989 (which is concerned with unauthorised disclosures of official information), the Government's "Protocol on Leak Investigations", procedural matters at trial, and miscellaneous unauthorised disclosure offences. Part III focuses on the protection the law requires to be afforded to disclosures that might be in the public interest.

1.30 We make numerous recommendations throughout this Report. These are then listed collectively in the final chapter. However, there are certain broad themes in the three parts of the Report that can be summarised here.

Part I: Espionage offences

1.31 In the first part of this Report, we recommend that a new, modernised espionage statute should replace the Official Secrets Acts 1911-1939. We make a number of specific recommendations about that proposed statute, which are designed to ensure that it addresses the nature of the threat now facing the UK. These include recommendations relating to the territorial ambit of the offences, replacing "enemy" with "foreign power", and the protection afforded to electronic data or programmes.

1.32 We note the proposals in the ISC's *Russia* report relating to the registering of foreign agents. However, these proposals did not form part of our consultation and thus we do not address them in this Report.[5]

---

5 Intelligence and Security Committee of Parliament, *Russia* (HC 632) para 114.

Part II: Unauthorised disclosure offences

1.33 This part addresses unauthorised disclosure offences, primarily under the Official Secrets Act 1989. We make many recommendations in this part, some substantive and some procedural. The following are of particular note:

(1) As with the offences in the 1911-1939 Acts, we make recommendations as to the territorial ambit of the 1989 Act offences.

(2) We recommend that the offences in sections 1-4 of the OSA 1989 (which apply only to public servants) that currently require proof of damage should no longer do so. (In accordance with the provisional proposals in our Consultation Paper, the offences in sections 5 and 6 (which apply to civilians) should continue to require proof of damage). This avoids the difficulties inherent in proving damage without disclosing further confidential information. Further, in Part III we have proposed a public interest disclosure mechanism, including a public interest defence, that would enable a defendant to establish that his or her disclosure was in the public interest *despite* any damage caused: we therefore consider that this affords better protection to the public interest than a damage requirement.

(3) We also recommend that certain disclosures for the purpose of seeking legal advice should be authorised disclosures under the terms of the OSA 1989, subject to the lawyer having the requisite security clearance and having undergone systems/premises assurance.

(4) Recognising that the scope for damage following an unauthorised disclosure is now many times greater than at any point in the past, we recommend that the maximum sentence be reviewed to ensure that it adequately addresses the most serious cases. Whilst we are recommending a review of the maximum sentence, we do not recommend any particular sentence; this is for Parliament to determine.

Part III: Public interest disclosures

1.34 One particular challenge in this Report has been to ensure that our recommendations afford protection to official data while also ensuring that the UK meets its obligations under Article 10 of the ECHR. In any case, there is an important balance to be struck between two competing public interests: in national security on the one hand and in accountable government on the other.

1.35 The right to freedom of expression is not absolute – it is qualified – and a clear inference can be drawn from the established case law under the ECHR that different considerations apply depending on whether the individual concerned is a public servant or a civilian.

1.36 The State has a broader discretion (often termed as “margin of appreciation”) to interfere with the Article 10 rights of public servants[6] (who owe a duty of loyalty, reserve and discretion) than it does when interfering with the rights of civilians

[6] Crown servants, government contractors, and notified persons, whether or not members of the security services.

(including, for example, journalists). Given the absence of a prior duty of loyalty, members of the public will likely be afforded greater latitude under the ECHR than public servants in the exercise of their Article 10, freedom of expression, rights.

1.37 As we explain in detail in the Report, we have concluded that not every prosecution that could currently take place under the existing OSA 1989 would be clearly compatible with Article 10 of the ECHR. We have therefore recommended that there should be two changes to the law.

1.38 First, we recommend that a statutory public interest defence should be created for civilians, including journalists, that they can rely upon in court. We consider that the defence should succeed only if the court finds that the disclosure was in fact in the public interest. This necessitates a two-stage analysis: first, whether the subject matter of the disclosure was in the public interest; and, secondly, whether the manner of disclosure was in the public interest. We also explain our view that the legal burden of proving the defence should rest on the defendant, and that this is not precluded by Article 6 of the ECHR (right to a fair trial). Beyond this basic structure, we do not recommend the detail of any public interest defence (such as which factors define the "public interest"), as we regard this as a political matter for Government and, ultimately, Parliament to determine in any legislation.

1.39 Secondly, in relation to public servants the position is different. The primary concern in respect of public servants is that there should be an effective investigative mechanism for addressing their concerns of illegal wrongdoing. The ECHR will afford protection to public servants' Article 10 rights in respect of unauthorised public disclosures only to the extent that such disclosures were necessary and a last resort. Accordingly, we have concluded that for public servants there should be created in statute a procedural mechanism whereby their concerns about possible wrongdoing can be investigated effectively. This would take the form of an independent commissioner to receive and investigate complaints of serious wrongdoing where disclosure of the matters referred to may otherwise constitute an offence under the Official Secrets Act 1989. That commissioner would also be responsible for determining appropriate disclosure of the results of that investigation. We also consider that, whilst such a truly effective independent investigative mechanism will suffice in most cases to ensure adequate protection of the rights of a public servant under Article 10 ECHR, it is possible to identify cases, albeit rare and exceptional, where such a process would not be sufficient. We therefore consider that there should be a residual statutory public interest defence for public servants upon which they can rely in court.

1.40 We acknowledge that the position we have adopted in this final report differs significantly from the provisional position we adopted in our Consultation Paper. This is due to the detailed and persuasive submissions and analysis we received during the consultation process which led us to alter our view on the benefits of a public interest defence.

ACKNOWLEDGEMENTS

1.41 In producing this Report, we have been fortunate in having assistance from many individuals and organisations. We are particularly grateful for time and efforts of the Law Commission staff who worked on the Report: Dr Nicholas Hoggard (team lawyer); David Connolly (team manager); Dr Karl Laird (lawyer in the early stages of the

Report); Dr Oliver Butler (lawyer in the early stages of the Report); Tatiana Kazim (research assistant); Alex Davidson (research assistant in the early stages of the Report); and Amy Woolfson (research assistant in the early stages of the Report).

1.42 We also acknowledge and thank Professor David Ormerod QC who was Commissioner of Criminal Law prior to the appointment of Professor Penney Lewis. Without Professor Ormerod's insight and guidance during the pre-consultation, consultation, policy development and early writing stages of this Report, this project could never have reached completion. The final recommendations should not be taken to represent Professor Ormerod's views.

PART I

Espionage Offences

Chapter 2: The Official Secrets Acts 1911-1939 and the Criminal Law's Response to Espionage

INTRODUCTION

2.1 We examined the Official Secrets Acts 1911-1939 in Chapter 2 of our Consultation Paper, asked a series of consultation questions, and put forward a number of provisional conclusions. As this was a Consultation Paper, we reached no final conclusions and made no recommendations to Government.[7]

2.2 Some of the responses to our Consultation Paper demonstrated common misunderstandings about the breadth of the current law. The offences in the Official Secrets Acts 1911-1939 are very wide but rarely prosecuted. The drafting is dated and obscure, and the supporting case law can be complex. It is thus not surprising that these offences are poorly understood. In this Chapter, therefore, we summarise the current law and provide some examples to demonstrate its application. In the next Chapter we turn to consider how the law should be reformed.

2.3 It was emphasised to us at a number of consultation events that the impact of the internet cannot be ignored in this context. The ubiquity of digital information storage and internet use has changed the nature of espionage, as it has many other areas of modern life. We therefore examine the offences contained in the Computer Misuse Act 1990, developing the points raised in the Consultation Paper. We also briefly examine how the Network and Information Systems Regulations 2018 have introduced greater protection for the United Kingdom's critical national infrastructure.

HISTORICAL OVERVIEW

The Official Secrets Act 1911

2.4 As we discussed in our Consultation Paper, the United Kingdom experienced outbreaks of both unauthorised disclosures and espionage during the late 19th century.[8] These were the catalysts for the enactment of the Official Secrets Act 1889 ("OSA 1889"). The Bill of 1889 was introduced into the House of Commons by the Attorney General and contained numerous provisions that criminalised both espionage and unauthorised disclosures. The OSA 1889 was criticised on the basis that it imposed a difficult burden on the prosecution and contained inadequate enforcement powers.[9]

2.5 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.[10]

---

7 We ought to have made this clearer since some consultees were under the impression we had concluded our work and recommended a new Espionage Act.

8 R Thomas, *Espionage and Secrecy* (1991) p 3; Consultation Paper, para 2.10.

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

10 R Thomas, *Espionage and Secrecy* (1991) p 12; Consultation Paper, para 2.11.

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 OSA 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 Secretary of State for War.[11]

2.6 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 subject to very little scrutiny by Parliament. The Bill's expedited passage was described in Parliament as "distressing" and "undesirable".[12]

Official Secrets Act 1920

2.7 The Official Secrets Act 1920 ("OSA 1920") amended the Official Secrets Act 1911 ("OSA 1911") and introduced new offences. It introduced evidential presumptions that apply in relation to prosecutions for offences contrary to section 1 of the OSA 1911. It also made permanent certain wartime provisions that were deemed necessary to make the OSA 1911 more effective.[13] A number of the 1920 Act provisions made it easier for the prosecution to prove certain elements of the offences in the OSA 1911. The OSA 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 improve the provisions of the OSA 1911 which had become ineffective in practice due to more modern methods of spying then being adopted.[14]

2.8 Thomas is particularly critical of the OSA 1920 on the grounds 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 reorganise the existing and new provisions into a clearer and more logical framework.[15]

2.9 In addition to amending the OSA 1911 and introducing the presumptions contained in section 2, the OSA 1920 contains a number of freestanding offences.[16]

---

11 *Hansard* (HL), 25 July 1911, vol 9, cc 641 to 647.

12 *Hansard* (HL), 18 August 1911, vol 29, cc 2257; Consultation Paper, para 212.

13 R Thomas, *Espionage and Secrecy* (1991) pp 11 to 34; Consultation Paper, para 2.74.

14 See R Thomas, *Espionage and Secrecy* (1991) pp 12 to 20.

15 R Thomas, *Espionage and Secrecy* (1991) pp 12 to 13; Consultation Paper, para 2.76.

16 eg: Unauthorised use of uniforms; falsification of reports, forgery, personation, and false documents: Official Secrets Act 1920, s 1 and Interfering with officers of the police or members of His Majesty's forces: Official Secrets Act 1920, s 3; Consultation Paper, para 2.77.

Official Secrets Act 1939

2.10 In 1937, a journalist named Ernest Lewis was convicted under section 6 of the OSA 1920 for failing to name the source who had passed him official information.[17] In 1938, section 6 was used by the Attorney General to question Duncan Sandys MP about his sources of information concerning the inadequacies of the air defences around London.[18] These two events highlighted the breadth of section 6 of the OSA 1920 and led to calls for reform. The Official Secrets Act 1939 ("OSA 1939") substituted a new section 6 in the OSA 1920. Section 6 of the OSA 1920 originally imposed a duty to give information relating to the commission of any offences under the Official Secrets Acts. The OSA 1939 amended the section so that the duty only applies in respect of offences contrary to section 1 of the OSA 1911.

SUMMARY OF CURRENT LAW AND EXAMPLES

2.11 The OSA 1911 contains two major types of espionage offence, which for convenience we have termed "espionage by trespass/proximity" and "espionage by information gathering/communication". These two types of offence are supplemented by other offences and investigatory powers in the OSA 1911 and 1920. In this section we give an overview of the offences relating to (a) espionage by trespass/proximity and (b) espionage by information gathering/communication.

Espionage by trespass/proximity

2.12 The offence of espionage by trespass/proximity is contained in section 1(1)(a) of the OSA 1911:

> (1) If any person for any purpose prejudicial to the safety or the 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;
>
> […]
>
> he shall be guilty of felony.

2.13 It is worth noting that the offence applies to "any person", and is not confined to "spies". This can be contrasted with the offences contained in sections 1 to 4 of the Official Secrets Act 1989, which can only be committed by Crown servants, government contractors, or notified persons. Further, by way of illustration, a

---

17 Prior to amendment by the 1939 Act, section 6 of the OSA 1920 read:

"It shall be the duty of every person to give on demand to a chief officer of police, or to a superintendent or other officer of police not below the rank of inspector appointed by a chief officer for the purpose, or to any member of His Majesty's forces engaged on guard, sentry, patrol, or other similar duty, any information in his power relating to an offence or suspected offence under the principal Act or this Act, and, if so required, and upon tender of his reasonable expenses, to attend at such reasonable time and place as may be specified for the purpose of furnishing such information, and, if any person fails to give any such information or to attend as aforesaid, he shall be guilty of a misdemeanour."

18 R Thomas, *Espionage and Secrecy* (1991) p18; Consultation Paper, para 2.95.

"prohibited place" could include, for example, military bases, nuclear fuel sites, or a government communications station.[19]

2.14 Whether the defendant regarded his or her purpose as being to prejudice the safety or interests of the state is not determinative of his or her criminal liability for this offence. The question for the jury is whether the defendant's purpose was, examined objectively, prejudicial to the safety or interests of the state.[20] It is not necessary for the defendant to enter the prohibited place, to cause any disruption to the operations of the prohibited place, or to take any particular action at the prohibited place, such as take a photograph. The penalty for this offence is a maximum of 14 years' imprisonment.[21]

Examples of current law

2.15 J is arrested outside a military base carrying high-powered binoculars. She is charged under section 1(1)(a) of the OSA 1911.

(1) J was bird watching, and had only a vague idea that there was a military base nearby. The jury could not, on that evidence, find that her purpose was prejudicial to the interest of the state. Clearly, she is not guilty of the offence.

(2) J is a helicopter enthusiast and approached the base in the hope of seeing new sorts of military helicopters. Her guilt depends on whether her purpose – to observe military helicopters – is, when objectively assessed by the jury, in their view prejudicial to the safety or interests of the state.

(3) J admits approaching the base with a view to watching what was going on, knowing that it was a military installation. However, she argues that she had reason to believe that crimes were being committed on the base and hoped to expose them. Her guilt depends on whether her purpose – to observe activity on a military base with a view to making it public – is, when objectively assessed by the jury, in their view, prejudicial to the safety or interests of the state.

(4) J is employed by a foreign government to observe and report on activity around UK military bases. She is guilty of the offence. Her purpose is, when objectively viewed, clearly prejudicial to the safety or interests of the state.

---

19 We address the list of prohibited places at para 3.70.

20 *Chandler v DPP* [1964] AC 763; Consultation Paper, para 2.27.

21 Official Secrets Act 1920, s 8(1); Consultation Paper, para 2.18.

Espionage by information gathering/communication

2.16 The offences of espionage by information gathering/communication are contained in section 1(1)(b) and 1(1)(c) of the OSA 1911. The sections provide:

> (1) If any person for any purpose prejudicial to the safety or the interests of the State –
>
> (a) […]
>
> (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.

2.17 As with espionage by trespass/proximity, there is no restriction on who can commit the espionage by information gathering/communication offences contained in section 1(1)(b) and 1(1)(c) of the OSA 1911. These offences can be committed by members of the public, journalists and government officials.

2.18 It is also worth underlining that the section does not apply only to "spies", as that term is commonly understood (although the section is entitled "penalties for spying"). Anyone who engages in the prohibited conduct, including a journalist, is treated as a spy for the purposes of this section, provided their purpose is objectively assessed to be prejudicial to the safety or interests of the state. During our consultation it became increasingly clear that this was a misunderstood feature of the offence. The offence labels certain types of conduct as "spying" even though the person who engages in that conduct may not consider themselves to be a spy, and even though his or her conduct may not be the type of conduct that is commonly understood to constitute spying.

2.19 Once again, whether the defendant's purpose was to prejudice the safety or interests of the state is an objective question that is decided by the jury on the facts of each case. Whether the defendant intended the conduct to prejudice the safety or interests of the state is not determinative of his or her criminal liability.

2.20 It is not necessary for the defendant's conduct to take place in a prohibited place. Furthermore, it is not necessary for there to be actual communication with an enemy, for an enemy to be identified, or for any communication to be useful to an enemy. These factors may form part of the evidence presented at trial, and may be relevant to sentencing.

2.21 As above, the offence carries a maximum sentence of 14 years' imprisonment.[22]

---

[22] Official Secrets Act 1920, s 8(1); Consultation Paper, para 2.18.

Example

2.22 K is a university lecturer specialising in radar technology. K is contacted by L who says he is an undergraduate interested in pursuing a similar career. In fact, L is an agent of a foreign power. Over coffee, K tells L that the government is very interested in a particular aspect of his research. K is prosecuted under section 1(1)(c) of the OSA 1911.[23] K accepts that he should not have shared this information but argues that his intention was to impress L and to encourage him to continue with his studies. Under the current law, K's perception of the legitimacy of his intention is not what matters. If the jury finds that K's purpose – based on an intention to share sensitive information with L – was objectively prejudicial to the safety or interests of the state, he will be convicted. L has also potentially committed an offence, if the jury find that he, having obtained information, did so intending that it be useful to an enemy with a purpose prejudicial to the safety or interests of the state.

Other criminal offences protecting sensitive sites

2.23 There is no general offence of trespass in the criminal law. It is important to note, however, that the offence contained in section 1(1)(a) of the OSA 1911 operates within a broader context of offences which criminalise trespass on certain sensitive sites or for certain purposes. These include aggravated trespass under section 68 of the Criminal Justice and Public Order Act 1994, which creates an offence of trespassing with the intention of intimidating persons so as to deter lawful activity, or intending to obstruct or disrupt that activity. Section 68 of the Criminal Justice and Public Order Act 1994 has been used to prosecute anti-war protestors who have caused disruption at military bases. For example, in 2002-2003 a group of protestors entered RAF Fairford as trespassers, intending to disrupt the operation of bomber jets stationed there.[24]

2.24 Under section 128 of the Serious Organised Crime and Police Act 2005 a person commits an offence if he or she enters, or is on, any "protected site" in England, Wales or Northern Ireland as a trespasser. As we explained in our Consultation Paper, a protected site is defined as a nuclear site or a designated site.[25] Nuclear sites are those on which premises subject to a nuclear site licence are located. Sites that have been designated by the Secretary of State include a number of military bases.[26] Other designated sites include the Palace of Westminster and the Ministry of Defence headquarters.[27] It is a defence for a person charged with an offence under

---

23 For these purposes it does not matter whether K is a government contractor or subject to any notification or vetting procedures.

24 See: A Phillips, *Gloucestershire Constabulary: Review of Operation Merit* (12 August 2004), available at https://www.gloucestershire.police.uk/media/2189/policing-of-raf-fairford-during-the-iraq-conflict.doc. The case of *R (Laporte) v Chief Constable of Gloucestershire* [2006] UKHL 55; [2007] 2 AC 105 related to separate, planned protests in March 2003 at RAF Fairford.

25 Serious Organised Crime and Police Act 2005, s 128(1A); Consultation Paper, para 2.157.

26 See, for example, the Serious Organised Crime and Police Act 2005 (Designated Sites) Order 2005/3447.

27 Serious Organised Crime and Police Act 2005 (Designated Sites under Section 128) Order 2007/930.

this section to prove that he or she did not know, and had no reasonable cause to suspect, that the site in relation to which the offence is alleged to have been committed was a protected site.[28]

2.25 Other trespass offences include trespassing on land forming part of a licensed or authorised aerodrome[29] and trespass on railway lines, amongst others.[30]

THE CRIMINAL LAW'S PROTECTION AGAINST CYBER ESPIONAGE

2.26 As with many crimes, the continued development of the internet has created new opportunities and methods for espionage. Hostile actors use the internet both as a tool for reconnaissance and a medium through which to conduct operations which threaten the safety and interests of the state.[31]

2.27 The offences contained in sections 1(1)(b) and 1(1)(c) of the OSA 1911 can be committed remotely by computer. For example, an individual who gains unauthorised access to Government computing systems to extract a list of security agents' home addresses would be recording information which might be useful to an enemy, contrary to section 1(1)(c) of the OSA 1911. This would also amount to an offence under the Computer Misuse Act 1990 ("CMA 1990"), to which we now turn.

2.28 The CMA 1990, as amended, provides the primary legislative protection for computer networks in the United Kingdom. In this section, we examine the CMA 1990 in brief and consider its relevance to the protection of official data.[32] We believe it important to set out these offences because some stakeholders expressed the view that our Consultation Paper paid insufficient attention to cyber espionage.

2.29 One common feature of the offences contained in the CMA 1990 is their broad territorial ambit. Any individual can commit these offences anywhere in the world and regardless of their nationality – provided there is a "significant link" between their conduct and the United Kingdom.[33] Section 5 of the CMA 1990 defines "significant link" in a number of ways. Where an unauthorised act is done in relation to a computer that is located within the United Kingdom, an offence is committed regardless of where the defendant was located at the time he or she gained unauthorised access to it. A computer hacker anywhere in the world commits an offence under the CMA 1990 if he or she accesses or attempts to gain unauthorised access to a computer in London, even though he or she may never have visited the United Kingdom.

Unauthorised access to computer material

2.30 Section 1 of the CMA 1990, as amended, provides:

---

28 Serious Organised Crime and Police Act 2005, s 128(4).

29 Civil Aviation Act 1982, s 39.

30 British Transport Commission Act 1949, s 55.

31 HM Government, *National Cyber Security Strategy 2016-2021*(November 2016) p 18.

32 For a more detailed analysis, see for example A Lloyd, *Information Technology Law* (OUP 2017) and A Murray, *Information Technology Law: The Law and Society* (3rd edn, OUP 2016).

33 In this respect the offences are wider in their territorial ambit than the 1911 Act.

(1) A person is guilty of an offence if—

(a) he causes a computer to perform any function with intent to secure access to any program or data held in any computer;

(b) the access he intends to secure is unauthorised; and

(c) he knows at the time when he causes the computer to perform the function that that is the case.

(2) The intent a person has to have to commit an offence under this section need not be directed at—

(a) any particular program or data;

(b) a program or data of any particular kind; or

(c) a program or data held in any particular computer.

2.31 The offence is triable either way.[34] When tried on indictment, the maximum sentence is two years' imprisonment.

Example 1

2.32 D hacks into the computer system at a military airbase. Having gained access to the system, D views data about patrol rotas. D has committed an offence contrary to section 1 of the CMA 1990.

Example 2

2.33 E, a cleaner at a military airbase, attempts to guess the password on the computer in the room he is cleaning. E intends to gain access in order to view the patrol rotas. E is unable to guess the password and so does not gain access to the computer. Nonetheless, E has committed an offence under section 1 of the CMA 1990.

Unauthorised access with intent to commit/facilitate further offences

2.34 Section 2 of the CMA 1990 states:

(1) A person is guilty of an offence under this section if he commits an offence under section 1 above ("the unauthorised access offence") with intent—

(a) to commit an offence to which this section applies; or

(b) to facilitate the commission of such an offence (whether by himself or by any other person);

[34] An "either way" offence is one that can be tried either in the Magistrates' Court or in the Crown Court.

and the offence he intends to commit or facilitate is referred to below in this section as the further offence.

2.35 The "further offences" to which the section applies are those for which the sentence is fixed by law,[35] or for which a person over 21 with no previous convictions may be sentenced to imprisonment for a term of five years. Therefore, this includes the offences contrary to section 1 of the OSA 1911.

2.36 The offence is triable either way. The maximum sentence, when tried on indictment, is five years' imprisonment.

Example

2.37 D hacks into the computer system at a military airbase. Having gained access to the system, D views data about patrol rotas. D has committed an offence contrary to section 1 of the CMA 1990. D's intention, in viewing this data, is to identify a time when it will be possible physically to enter the base without being apprehended. D has committed an offence contrary to section 2 of the CMA 1990 as he has committed the section 1 offence with the intention to commit/facilitate a further offence, in this instance an offence contrary to section 1 of the OSA 1911.[36]

Unauthorised acts with intent to impair or recklessness as to impairment of a computer

2.38 Section 3 of the CMA 1990, as amended, states:

(1) A person is guilty of an offence if –

(a) he does any unauthorised act in relation to a computer;

(b) at the time when he does the act he knows that it is unauthorised; and

(c) either subsection (2) or subsection (3) below applies.

(2) This subsection applies if the person intends by doing the act –

(a) to impair the operation of any computer;

(b) to prevent or hinder access to any program or data held in any computer; or

(c) to impair the operation of any such program or the reliability of any such data.

---

35 eg, murder.

36 D has also committed an offence contrary to section 7 of the Official Secrets Act 1920.

(3) This subsection applies if the person is reckless as to whether the act will do any of the things mentioned in paragraphs (a) to (c) of subsection (2) above.

(4) The intention referred to in subsection (2) above, or the recklessness referred to in subsection (3) above, need not relate to -

(a) any particular computer;

(b) any particular program or data; or

(c) a program or data of any particular kind.

(5) in this section –

(a) a reference to doing an act includes a reference to causing an act to be done;

(b) "act" includes a series of acts;

(c) a reference to impairing, preventing or hindering something includes a reference to doing so temporarily.

2.39 The offence is triable either way. When tried on indictment, the maximum sentence is 10 years' imprisonment and/or a fine.[37]

2.40 This offence is relevant to acts of sabotage, and also to denial of service attacks.[38]

Example

2.41 D hacks into the computer system at a military airbase. Having gained access to the system, D views data about patrol rotas. Having viewed the data, D deletes it from the airbase's computer system. D has committed an offence contrary to section 3 of the CMA 1990.

Impairing a computer such as to cause serious damage

2.42 Section 3ZA of the CMA 1990[39] provides:

(1) A person is guilty of an offence if –

(a) the person does any unauthorised act in relation to a computer;

(b) at the time of doing the act the person knows that it is unauthorised;

---

37 Criminal Misuse Act 1990, s 3(6)(c).

38 An interruption in an authorised user's access to a computer network, typically one caused with malicious intent.

39 Inserted by section 41 of the Serious Crime Act 2015.

(c) the act causes, or creates a significant risk of, serious damage of a material kind; and

(d) 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.

(2) Damage is of a "material kind" for the purposes of this section if it is –

(a) damage to human welfare in any place;

(b) damage to the environment of any place;

(c) damage to the economy of any country; or

(d) damage to the national security of any country.

(3) For the purposes of subsection (2)(a) an act causes damage to human welfare only if it causes –

(a) loss to human life;

(b) human illness or injury;

(c) disruption of a supply of money, food, water, energy or fuel;

(d) disruption of a system of communication;

(e) disruption of facilities for transport; or

(f) disruption of services relating to health.

(4) It is immaterial for the purposes of subsection (2) whether or not an act causing damage –

(a) does so directly;

(b) is the only or main cause of the damage.

(5) In this section –

(a) a reference to doing an act includes a reference to causing an act to be done;

(b) "act" includes a series of acts;

(c) a reference to a country includes a reference to a territory, and to any place in, or part or region of, a country or territory.

2.43 The offence is triable on indictment only and carries a maximum sentence of life imprisonment in the context of a threat to life, loss of life or damage to national security, or 14 years' imprisonment in all other instances.[40]

2.44 This is a broad offence, as the defendant's unauthorised act does not have to cause serious damage of a material kind. It is sufficient for the act to create a *significant risk* of causing serious damage of a material kind.

Example

2.45 D introduces a virus into the computer system controlling a mobile communications network. This causes large sections of the network to fail for a brief period. D has committed an offence contrary to section 3ZA of the CMA 1990, which carries a maximum penalty of 14 years' imprisonment.

2.46 C launches a denial of service attack at a large NHS trust. Healthcare services are subject to major disruption. C has committed an offence contrary to section 3ZA of the CMA 1990, which carries a maximum penalty of life imprisonment.

ENSURING COMPUTER NETWORKS ARE ADEQUATELY PROTECTED

2.47 It is in the State's interests to reduce the risk of cyber-attacks by hostile agents which pose a risk to the safety or interests of the State. That is especially important in relation to computer systems that contain data relating to government. The most sensitive data is held by government in the most secure manner, but the range of government-related data that could be attacked is obvious – for example, that relating to critical national infrastructure.[41]

2.48 As we have seen, the CMA 1990 offences, as extended, criminalise a wide range of unauthorised conduct involving computer networks. These offences have now been augmented by the Network and Information Systems Directive, which was promulgated in 2016 by the European Union. In the United Kingdom, the Directive has been implemented into domestic law by the enactment of the Network and Information System Regulations 2018 ("the 2018 Regulations") which came into force on 10 May 2018. According to the Explanatory Memorandum, the purpose of the 2018 Regulations is:

> To establish a legal framework to ensure that essential services and selected digital service providers within the UK put in place adequate measures to improve the security of their network and information systems, with a particular focus on those services which if disrupted, could potentially cause significant damage to the UK's

[40] Computer Misuse Act 1990, s 3ZA(6) and (7).

[41] There are in addition the offences under the Data Protection Act 2018 which are examined more fully in Chapter 6.

economy, society and individuals' welfare; and to ensure serious incidents are promptly reported to the competent authorities.[42]

2.49 The 2018 Regulations apply to operators of essential services across a range of industries in the private and public sectors. Every operator of essential services is required to take measures to improve their cyber security and to report breaches to the authorities. Failure to comply with the 2018 Regulations could result in fines of up to £17m.[43]

[42] See: Explanatory Memorandum to the Network and Information Systems Regulations 2018, para 2.1.

[43] See: Explanatory Memorandum to the Network and Information Systems Regulations 2018, para 8.3.

Chapter 3: The Official Secrets Acts 1911-1939: Recommendations for Reform

INTRODUCTION

3.1 In this Chapter we consider the problems with the Official Secrets Acts 1911-1939 and make recommendations for reform. We recommend that these Acts be repealed and replaced with a new statute governing espionage explicitly. As will be seen, the new offences we recommend modernise many aspects of the current offences, as well as remove redundant provisions. We retain, however, the two types of espionage offence: (i) espionage by trespass or observation; and (ii) espionage by collection and communication of information.

3.2 We present our analysis in this Chapter thematically. In the Consultation Paper we analysed the problems in the present law separately, dealing with each statutory provision in turn. Whilst many consultees followed the format of the Consultation Paper in their responses, others chose to respond more thematically. On reflection, the topic seems better suited to a thematic analysis rather than an analysis of each provisional proposal in turn: many consultation questions and provisional conclusions were designed to be read cumulatively. We have therefore chosen to group our analysis and recommendations in this chapter by theme. We hope this will make our recommendations clearer and easier to follow.

A NEW STATUTE

Replacing the Official Secrets Acts 1911-1939 with a new statute

3.3 In our Consultation Paper we asked consultees whether they agreed that the Official Secrets Acts 1911-1939 ought to be repealed and replaced with a new statute. We suggested that this would provide an opportunity to ensure that the offences were fit for purpose for the modern age. We also suggested that a new statute would provide an opportunity to relabel the legislation so that it referenced espionage explicitly.

Provisional conclusion 8

3.4 Provisional conclusion 8 stated:

> We provisionally conclude that the Official Secrets Acts 1911-1939 ought to be repealed and replaced with a single Espionage Act. Do consultees agree?[44]

Consultation responses

3.5 Consultees who agreed with provisional conclusion 8 included Dr Ashley Savage, Peters and Peters, and the Bar Council and Criminal Bar Association. The Crown Prosecution Service expressed concern that "while some amendments to the current

[44] Consultation Paper, p 49.

1911-1939 Acts might get through Parliament, to suggest a complete re-enactment would not be practical".[45]

3.6 Individual consultee Sue Jackson commented that "although it is inevitable that some of the language used … is out of date, the danger in repealing and replacing existing law is that the scope of the legislation may be extended in ways which are prejudicial to the functioning of a healthy democracy".[46]

3.7 Consultees representing the media disagreed with this provisional conclusion, on the basis that any attempt at reform would invariably lead to further restrictions on the free communication of information. The point was made that if there was an intention to repeal and replace the Official Secrets Acts 1911-1939, the process would need to be prefaced by extensive engagement with media organisations, to ensure that any new legislation did not place further restrictions on journalists' ability to communicate stories in the public interest.

3.8 We continue to see the merits in a modern statute dealing with espionage, stripped of archaic language and outdated assumptions. For clarity, we include at the end of this chapter a table comparing the current offences with the recommended provisions.

Recommendation 1.

3.9 We recommend that a new statute – containing modern language and updated provisions – should replace the Official Secrets Acts 1911-1939.

PROBLEMS WITH THE CURRENT LAW

3.10 In this section, we outline the problems we identified with the 1911-1939 Acts in our Consultation Paper. We set out and analyse consultees' responses to our consultation questions and provisional conclusions. At the end of each section we provide our recommendations to Government. We also consider the supplementary offences and powers contained in the Official Secrets Acts 1911 and 1920.

Replacing "enemy" with "foreign power"

3.11 As discussed in Chapter 2, section 1(1)(b) and 1(1)(c) of the Official Secrets Act 1911 ("OSA 1911") provide that it is an offence for a person to make or obtain "any sketch, plan, model or note", or obtain "any secret official code word, or pass word … 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".[47]

3.12 In our Consultation Paper we argued that the use of the word "enemy" in this section of the OSA 1911 is problematic, for the following reasons:

---

45 Crown Prosecution Service, p 4.

46 Sue Jackson, by email.

47 Consultation Paper, para 2.106.

(1) as noted over a decade ago by the Intelligence and Security Committee of Parliament, the word "enemy" raises problems of construction, and of "giving unnecessary offence to states with which the UK is not at war";[48] and

(2) as a term that was drafted with enemy states in mind, it is unclear whether a court would construe "enemy" broadly enough to encompass non-state actors, such as an international terrorist group.[49]

3.13 We noted that simply replacing the word "enemy" with another term without making any further changes to the language of section 1 would risk upsetting the balance of the offence and would risk making it overly broad.[50]

Provisional conclusion 1

3.14 Provisional conclusion 1 stated:

> 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?[51]

3.15 Having identified deficiencies with the term "enemy", we suggested that the definition of "foreign power", as adopted by the United States Espionage Statutes Modernization Bill, might provide a more suitable basis for a modern espionage offence.[52] The term "foreign power" in the Bill was to be given the meaning contained in section 101 of the United States 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

---

48 Intelligence and Security Committee: Annual Report 2003-2004 (2004) CM 6240, p 43; Consultation Paper, para 2.109.

49 Consultation Paper, para 2.112.

50 Consultation Paper, para 2.115.

51 Consultation Paper, para 2.113.

52 Consultation Paper, para 2.141.

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

3.16 The Espionage Statutes Modernization Bill was introduced into the Congress of the United States in 2010. It was not enacted.

Consultation question 3

3.17 We did not suggest that the definition ought to be incorporated wholesale into UK law, but that it might provide a useful "starting point" as to how the word "enemy" could be defined in a replacement offence.[53]

3.18 Consultation Question 3 asked:

> 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?[54]

Consultation responses

3.19 A number of consultees, including the Crown Prosecution Service, the Bar Council and Criminal Bar Association (who submitted a joint response), Oliver Butler[55] and Peters and Peters agreed with provisional conclusion 1. The Crown Prosecution Service added:

> We agree that the potential replacement term 'foreign power' would appear to be sufficient and that the wording would need to be wide enough to make the offence apply to UK residents, not simply British citizens.[56]

3.20 Those who disagreed, including Guardian News and Media and ITN, argued that "foreign power" was a broader term that could lead to the reformulated offence capturing behaviour that was not espionage. Guardian News and Media gave the following example:

> …if a journalist obtains information that a nuclear defence installation is unsafe, that concerns have been reported to the appropriate authorities, but have been discounted, and the journalist then proceeds to investigate whether the information is true, they should not be placed at risk of prosecution. Under the existing wording of section 1 OSA the 'of use to the enemy' requirement would it is submitted make such a prosecution unlikely, however if that wording were changed to a foreign power, and a foreign state-owned institution was thinking of bidding to

---

53 Consultation Paper, paras 2.139 to 2.143.

54 Consultation Paper, para 2.144.

55 Dr Oliver Butler is now a barrister and a Fellow in Law at Wadham College, Oxford. He submitted a consultation response whilst a PhD student. He subsequently worked on aspects of this project as a consultant.

56 Crown Prosecution Service, p 2.

decommission the plant, this could catch the journalist. Such activity by a journalist should not be considered to be espionage.[57]

3.21 Similarly, ITN stated:

> Changing [enemy] to "foreign power" broadens the term far too much. This leads to lack of clarity on how to handle the passing of information by organisations such as NGOs or civil society groups. In the context of Brexit, as one example, a group could be accused of supporting EU positions or passing on information in negotiations. This activity is clearly not espionage and should not be treated as such – nor the information that they pass on to media. As a result of this proposed legislation anyone that published an intelligence- or foreign affairs-related story based on a leak would be open to criminal charges.[58]

3.22 There were fewer responses that specifically addressed consultation question 3. Peters and Peters agreed that the list of foreign entities contained in the Espionage Statutes Modernization Bill was a helpful starting point, as did Oliver Butler, who stated that "it clarifies that the offence would apply to all foreign governments, foreign political factions, entities directed or controlled by those governments".[59] Moreover, the Bar Council and Criminal Bar Association stated:

> The list of entities and organisations is a helpful starting point. It would not be unreasonable under (4) for the prosecution to be able to prove this element by reference to a non-exhaustive list of terrorist organisations designated by the state, in addition to defining "foreign power" so as to include, for example, nation states. Presumably there will be no requirement for the prosecution to prove which foreign power/organisation would benefit by the commission of the offence. It is agreed that in the domestic context the definition should refer to UK residents.[60]

3.23 The News Media Association stated:

> The very broad ranges of possible meanings of "foreign power" at 2.139 show how far the interpretation of such a substitution could extend, from business reporting to reporting of terrorism.[61]

Classified evidence

3.24 We have seen evidence in relation to the threats posed by hostile actors that would not meet the definition of "enemy". This evidence cannot be published in the public domain owing to the security classification. The following is a hypothetical example that illustrates the risks revealed by the classified evidence.

(1) P, an IT services company headquartered in a foreign state, has a managed services contract for a large government department. As part of this contract,

---

57 Guardian News and Media, p 43.

58 ITN, pp 4 to 5.

59 Oliver Butler, p 4.

60 The Bar Council and the Criminal Bar Association, para 25.

61 News Media Association, pp 18 to 19.

P creates backups in the UK of the department's corporate email and file storage system. P is compelled under the foreign state's national security legislation to share this information with the foreign state's intelligence services, who use it to target UK interests.

Analysis

3.25 By way of introduction, we agree with those consultees who expressed the view that, without further changes, replacing the term "enemy" with "foreign power" could make the offence too wide. It is for this reason that we provisionally proposed, and now recommend, a broader restructuring of the section 1 offence. We see considerable merit in the point made by the News Media Association about the potential problems that would be caused by the breadth of the definition of "foreign power" contained in the Espionage Statutes Modernization Bill. In relation to the example given by Guardian News and Media, we reiterate that the journalist in that scenario would only commit an offence if he or she acted with a purpose prejudicial to the safety or interests of the state. Furthermore, it is arguable that information relating to deficiencies with a nuclear defence installation is information that might be directly or indirectly useful to an enemy for the purposes of the existing offences.

3.26 We are persuaded by the concerns consultees raised about the inclusion of some of the entities contained in the Espionage Statutes Modernization Bill in the definition of "foreign power", and the reservations that it would lead to a very broad definition of the term. We believe, however, that there is a good case to be made for replacing the word "enemy". The challenge is to find a suitable replacement that would not render the offence overly broad.

3.27 Our view is that consultees' concerns can be met by ensuring that the definition of "foreign power" is sufficiently tightly drawn. A narrower definition of "foreign power" is used in Canadian law. That is, we consider, an option worth pursuing as a foundation for drafting a new form of the offences. We believe it would achieve the same policy objectives, but would meet the concerns consultees expressed about the need to ensure the offence is not overly broad.

3.28 Section 4(1)(b) of the Canadian Security of Information Act 2001 makes it an offence for a person to use certain types of information in their possession for the benefit of a foreign power or in any other manner prejudicial to the safety or interests of the state. Section 2(1) of the Act provides the following definition:

> ***Foreign power*** means:
>
> (a) The government of a foreign state,
>
> (b) An entity exercising or purporting to exercise the functions of a government in relation to a territory outside Canada regardless of whether Canada recognises the territory as a state or the authority of that entity over the territory, or
>
> (c) A political faction or party operating within a foreign state whose stated purpose is to assume the role of government of a foreign state …

3.29 We are not suggesting that this definition be incorporated wholesale into UK law, but believe that it could provide a useful starting point when considering how "foreign power" could be defined in legislation. It is narrower than the formulation we originally proposed. It also seems more accurately to reflect how espionage is typically conceptualised. We see merit in considering whether this Canadian definition ought to be broadened to encompass terrorist groups and entities that are directed and controlled by foreign governments.[62] Notably, Section 6 of the Canadian Security of Information Act 2001 provides that every person commits an offence who, for any purpose prejudicial to the safety or interests of the State approaches, inspects, passes over, is in the neighbourhood of or enters a prohibited place at the direction of, for the benefit of or in association with a foreign entity or terrorist group. The need to include the former, including those that are not recognised as state entities by the UK, seems to us to be self-evident. The latter requires more explanation.

3.30 As we noted in our Consultation Paper, there are examples of individuals who have committed espionage, although they were not acting directly for the benefit of a foreign government. Instead, such individuals were acting under the direction of entities controlled by a foreign government, such as a state-owned company. This is the situation reflected in the classified evidence we have seen (cited by way of example above at 3.24(1)). By way of further example, Allen Ho, a naturalised citizen of the United States, was indicted in the United States for running an espionage ring aimed at obtaining information relating to the nuclear industry. According to the indictment, Mr Ho was acting under the direction of a Chinese state-owned nuclear power company. We would therefore suggest drafting the definition to ensure that the offence applies to conduct relating to:

(1) a group engaged in international terrorism or activities in preparation thereof; and

(2) an entity that is directed and controlled by a foreign government.

3.31 As well as being more narrowly drawn than our original suggestion, the example taken from Canadian law has the advantage that it was specifically created with espionage offences in mind.[63] Should the Official Secrets Acts 1911-1939 be repealed and replaced, the merits of adopting this definition would need to be explored more fully with stakeholders.

---

62 Consultation Paper, para 2.115.

63 In contrast, the purpose of the US Foreign Intelligence Services Act 1978 is to provide a system for obtaining warrants to intercept the communications of people in the United States who are suspected of being agents of a foreign power.

Recommendation 2.

3.32 In any new statute to replace the Official Secrets Act 1911, the concept of "enemy" in section 1 should be replaced with that of "foreign power". The Canadian definition of "foreign power", including reference to terrorist groups and entities directed by a foreign government, should be used as a starting point for drafting that element of the new provision.

Replacing "safety or interests of the state" with "national security"

3.33 In our Consultation Paper we suggested replacing the words "safety or interests of the state" with "national security". Our contention was that agents of foreign powers routinely gather considerable amounts of information for the benefit of a foreign power with the intention of prejudicing the interests of the United Kingdom, but we suggested in our Consultation Paper that few people would consider that all such conduct should necessarily constitute the criminal offence of espionage.[64]

3.34 To address this concern, we asked whether the term "safety or interests of the state" should be replaced with the term "national security". In doing so, we noted that the term "national security" would bring the legislation more directly into alignment with the language used in the European Convention on Human Rights ("ECHR").[65]

Consultation question 1

3.35 Consultation question 1 asked:

> 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"?[66]

Consultation responses

3.36 While the majority of consultees' responses were opposed to any change, the Bar Council and Criminal Bar Association, amongst others, agreed with the proposition set out in this consultation question. They stated:

> The current wording should be replaced with "national security". It is a concept more readily capable of definition and it also serves to narrow the scope of the offence.[67]

3.37 The Crown Prosecution Service did not engage with this question as they thought that those in the intelligence community were better placed to answer it.[68]

3.38 Those consultees who opposed the change, including Guardian News and Media, ITN and Peters and Peters, argued that "national security" was even less well-defined

---

64 Consultation Paper, para 2.127.

65 Consultation Paper, para 2.128.

66 Consultation Paper, para 2.129.

67 The Bar Council and the Criminal Bar Association, para 16.

68 Crown Prosecution Service, p 2.

and/or potentially broader than "safety or interests of the state".[69] The News Media Association agreed that "narrowing 'safety or interests of the state' would be helpful, but more detailed consideration and consultation on the meaning and ambit of 'national security' or any other term substituted is necessary".[70] Individual consultee Annie Machon, a former intelligence officer, suggested that the lack of a definition in the United Kingdom of "national security" means that the concept is "effectively elastic, meaningless, and open to abuse".[71]

3.39 Peters and Peters expressed their concern in the following terms:

> If there is no definition set down in the legislation, "national security" could in practice become as broad as "safety or interests of the state". This is especially concerning when the information used to assess the risk of national security may not be made public during the course of any trial under the cover of public interest immunity. Prosecutions should be as transparent as possible and the public can have a greater confidence that the legislation will not be misused if the definition of national security is as precise as possible.[72]

3.40 ITN stated:

> The Law Commission does not provide any definition of the term "national security" despite suggesting that this term should replace the more specific wording "safety or interests of the state". This is not a like-for-like swap and simply introduces a different, wide-reaching and equally vague replacement.[73]

3.41 The Government Response agreed that "national security" was narrower than "safety or interests of the state", but argued that it would not be desirable to adopt such a narrow term. The Government Response stated:

> It is important that the law continues to protect the "safety or interests" of the UK and not only its security. Espionage against the UK is not conducted, and never has been, solely with the aim of prejudicing our national security. The experience of HMG [Her Majesty's Government] and the governments of allied states is that espionage is frequently targeted at and can do significant damage to important national interests that fall (or may fall) outside the scope of national security.[74]

Analysis

3.42 The difficulty we have faced in evaluating the responses to this provisional conclusion is exemplified by the fact that those consultees representing the media considered the term "national security" to be too broad, whilst the Government Response considered it to be too narrow. As we have already explained, the view we took in our

---

69 eg, see Guardian News and Media, p 44.

70 News Media Association, p 19.

71 Annie Machon, p 1.

72 Peters and Peters, p 2.

73 ITN, p 5.

74 Government Response, pp 3 to 4.

Consultation Paper was that the term "national security" is narrower than the term "safety or interests of the state".

3.43 The reason we did not provide a provisional definition of "national security" is that historically the term has been left undefined in statute.[75] We did not consider this to be fatal, as a matter of legal certainty, to whether the term could be used in the context of espionage. Whether the term "national security" is sufficiently precise to satisfy the ECHR was considered by the Grand Chamber of the European Court of Human Rights ("ECtHR") in *Kennedy v United Kingdom*.[76] Not only did the Grand Chamber conclude that the term was sufficiently precise to satisfy Article 8(2) of the ECHR but it also stated that: "by the nature of things, threats to national security may vary in character and may be unanticipated or difficult to define in advance." The flexibility of the term was seen by the ECtHR as an advantage.

3.44 We considered the term "national security" to encompass a narrower range of interests than the term "safety or interests of the state", but the vast majority of consultees disagreed with us. We acknowledge that, were the term to remain undefined, it is possible that it could be construed to encompass a broader range of interests than is currently encompassed by "safety or interests of the state". Consultees seemed to prefer the certainty that is provided by the current law. We can certainly see merit in this view and therefore recommend no change.

Recommendation 3.

3.45 In any new statute to replace the Official Secrets Act 1911, the term "safety or interests of the state" should be retained.

The fault element: purpose prejudicial

3.46 In our Consultation Paper, we examined the fault element of the offences contained in the OSA 1911: "purpose prejudicial".[77] How "purpose prejudicial" is interpreted is governed by the decision of the House of Lords in *Chandler v DPP*:[78]

3.47 The term "purpose" contains a subjective element, but is not wholly subjective. On the facts of *Chandler*, it was sufficient to prove that the defendants entered an airbase with the intention of disrupting it. Once it was proved that the defendants' intention was to disrupt the airbase, the further question of whether that amounted to a "purpose prejudicial to the safety or interests of the state" was an objective one, ie was their subjective purpose objectively prejudicial to the safety or interests of the state? The defendant's opinion as to whether their purpose was beneficial or prejudicial to the state is therefore irrelevant.

---

75 See, for example: Data Protection Act 1998, s 28 (no longer in force); Regulation of Investigatory Powers Act 2000; and Data Retention and Investigatory Powers Act 2014, s 3 and s 7.

76 *Kennedy v United Kingdom* (2001) 52 EHRR 4 at [159].

77 Consultation Paper, paras 2.26 to 2.28.

78 [1964] AC 763.

3.48 What is arguably the most important element of the section 1 OSA 1911 offence – prejudice to the safety or interests of the state – does not require the defendant subjectively to intend to prejudice the safety or interests of the state. In our Consultation Paper, we explained that when the term "purpose" is used to denote fault in the context of a criminal offence, it is typically understood to require a subjective evaluation of the defendant's state of mind.[79] For that reason, the understanding of "purpose" that has been adopted in the context of the OSA 1911 is unusual. Given the seriousness of the offence, we argued in our Consultation Paper that it was important for this element of the offence to incorporate a subjective fault element.

3.49 To achieve this aim, we asked whether the offence should be narrowed in this respect. Specifically, we asked whether 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. If the offence were to be amended in this way, the prosecution would have to prove that the defendant knew or had reasonable grounds to believe that his conduct might prejudice the safety or interests of the state. If this burden could not be discharged, then the defendant would be entitled to an acquittal.

Consultation question 2

3.50 Consultation question 2 asked:

> 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?[80]

Consultation responses

3.51 Evaluating the responses that we received to this consultation question proved to be difficult since a number of consultees did not appreciate that the term "purpose prejudicial" does not currently require a subjective evaluation of the defendant's state of mind. Of those consultees who did appreciate the context in which we were asking this consultation question, Campaign Against Censorship, News Group Newspapers and Peters and Peters all agreed that a subjective fault element should be introduced. News Group Newspapers also proposed:

> … that the standard is that the Defendant knew or had reasonable grounds to believe that their conduct "*would*" [rather than "*might*"] prejudice national security …[81]

3.52 Other consultees, such as Guardian News and Media, were in favour of introducing a subjective fault element in principle, but not at the cost of broadening other aspects of the offence.[82] The Crown Prosecution Service was against introducing a subjective

---

79 Consultation Paper, paras 2.27 to 2.28.

80 Consultation Paper, para 2.137.

81 News Group Newspapers, p 1.

82 eg, see Guardian News and Media, p 47.

fault element on the grounds that it could lead to a reduction in the number of prosecutions that are capable of being brought.

Analysis

3.53 Our consultation question referred to *conduct* (that D knew or had reasonable grounds to believe was prejudicial) rather than *purpose*. Whilst this was not the focus of the question (which instead concerned the subjective element), we nonetheless consider that "purpose" is preferable. This is because purpose includes those aims to which one's conduct is directed. If the inquiry were limited to "conduct", one would have to ask whether, for example, trespassing on a base could, in and of itself, reasonably be believed to prejudice the safety or interests of the state. What is important, though, is not the conduct itself, but the reason for the conduct. Therefore, we have reverted to use of the word "purpose" in the following recommendation.

3.54 We acknowledge the concern raised by the Crown Prosecution Service, but the requirement to prove subjective fault is often a feature of serious criminal offences. We continue to hold the view that it is undesirable for it to be possible to convict an individual for a highly stigmatising offence that carries a maximum sentence of 14 years' imprisonment, despite the fact he or she may not have possessed a culpable state of mind.

3.55 In relation to the concern raised by Guardian News and Media, we would stress once again that our intention is not to broaden aspects of this offence as they currently relate to journalism. The offences in the OSA 1911 are applicable to journalists in the same way that they are applicable to everyone else in the United Kingdom. One consequence of introducing a requirement to prove a culpable state of mind is that it should be less likely that a responsible journalist could be prosecuted, given that he or she would lack this state of mind.

Recommendation 4.

3.56 An individual should only be criminally liable for an espionage offence if he or she has a purpose which he or she knows or has reasonable grounds to believe is prejudicial to the safety or interests of the state.

The fault element: benefit to a foreign power ("useful to an enemy")

3.57 Under the current law, sections 1(1)(b) and 1(1)(c) of the OSA 1911 criminalise the collection and creation of types of information that may be useful to an enemy:

> (1) If any person for any purpose prejudicial to the safety or interests of the State –
>
> (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.

3.58 Taken at its broadest, a person would be guilty of an offence if, with a purpose prejudicial to the state (currently an objective test) they make a sketch which might be indirectly useful to an enemy. This is a low threshold for the prosecution to meet. We asked consultees for their views on whether a further fault element should be introduced in relation to the offences contained in sections 1(1)(b) and 1(1)(c) of the OSA 1911.

3.59 We recognised that it would be impractical to require the prosecution to prove that an enemy had in fact benefited from the defendant's conduct.[83] We did suggest, however, that it was problematic to have such an easily satisfied conduct element without requiring any knowledge or foresight as to whether a foreign power *might benefit* from the conduct. Our aim was to ensure that this element of the offence was accompanied by a corresponding fault element.

Provisional conclusion 3

3.60 Provisional conclusion 3 stated:

> 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 benefitting a foreign power. Do consultees agree?[84]

Consultation responses

3.61 A number of consultees agreed with this provisional conclusion, including Campaign Against Censorship. News Group Newspapers were also in agreement, but queried the different standards of knowledge and belief contained in consultation question 2 as opposed to provisional conclusion 3:

> News Group Newspapers proposes that the same standard is adopted for both offences [and] proposes that the standard is that the defendant knew or had reasonable grounds to believe that their conduct "*would*" … benefit a foreign power.[85]

3.62 The Bar Council and Criminal Bar Association agreed with the provisional conclusion, but questioned how it would work in practice:

> It is not clear though how it is that the prosecution will prove this element of the offence. Is it intended, for example, that it will be sufficient for the prosecutor to lead

---

83 Consultation Paper, para 2.147.

84 Consultation Paper, para 2.150.

85 News Group Newspapers, p 1.

evidence of the types of behaviour which it might reasonably be considered capable of benefitting foreign power?[86]

3.63 Peters and Peters gave qualified support, agreeing that the offence should contain a subjective fault element, but suggesting that "capable of" benefitting a foreign power was too low a bar:

> A remote possibility of future benefit would seem to suffice to establish fault under this wording.[87]

3.64 The Crown Prosecution Service did not respond to this provisional conclusion. Whilst some consultees argued that "capable" was too low a bar, others appeared to be working under the assumption that the current law requires proof of actual prejudice to the safety or interests of the state. The current law does not require such proof in order to secure a conviction, however. The Government Response stated:

> We believe the law would be too narrowly framed if it required the defendant to know or have reasonable grounds to believe that their conduct was capable of benefitting a foreign power. A requirement in those terms would enable a person who knew that their conduct was prejudicial to the UK to escape prosecution for espionage on the basis that although they suspected they might be dealing with a foreign power, there were in fact no grounds on which they could reasonably believe that to be the case…we therefore consider the law should require the defendant to know or have reasonable grounds to believe that they are dealing with a foreign power, or to suspect that they may be.[88]

3.65 Liberty submitted that this provisional conclusion was "reached with little analysis or discussion" and "accompanied by the unevidenced claim" that requiring the prosecution to prove that the defendant's conduct did in fact benefit a foreign power could be very difficult.[89]

3.66 Professor David Leigh, Anthony Sampson Professor in Reporting at City, University of London disagreed with the provisional conclusion, "on the grounds that it will open the way to the criminalisation of bona fide journalists for allegedly 'spying'".[90]

Analysis

3.67 Provisional conclusion 3 in the Consultation Paper was designed to add a further subjective fault element in relation to the offences under sub-sections 1(1)(b) and 1(1)(c) of the OSA 1911. It was designed to limit the reach of the offence.

3.68 However, having reflected on consultees' views, and how the test would operate in practice, we consider that, so long as there is a wholly subjective fault element, it is sufficient to have proof of subjective fault as to the prejudice to the safety or interests of

---

86 The Bar Council and Criminal Bar Association, p 6.

87 Peters and Peters, p 3.

88 Government Response, p 5.

89 Liberty, p 11.

90 Professor David Leigh, by email.

the state, without requiring further proof that this serious malintent was also intended to be capable of benefitting a foreign power. In any case, it is not clear how one can intend conduct prejudicial to the safety or interests of the state without intending that it be *capable* of benefitting a foreign power. That said, as the Bar Council and Criminal Bar Association noted, requiring the prosecution to prove that the defendant had intent as to this second element of the offence would introduce problems of proof that could be very difficult to meet.

3.69 As such, we have concluded it is sufficient for this component of the offence to be objective, and for the jury to be sure that the defendant's conduct was capable of benefitting a foreign power.

Recommendation 5.

3.70 In any new statute to replace the Official Secrets Act 1911, the requirement that the defendant's conduct was capable of benefitting a foreign power should continue to be objectively determined. There should be no requirement to prove that the defendant personally knew or believed that his or her conduct had such capability.

The list of prohibited places

3.71 The list of prohibited places in section 3 of the OSA 1911 has a strong military focus. This is unsurprising given the background to its enactment in 1911 which we described in Chapter 2. The Secretary of State has the power to make an order declaring further sites to be prohibited places. However, this power has been exercised infrequently in practice.

3.72 As we discussed in our Consultation Paper, our pre-consultation engagement with stakeholders from various government departments suggested that the list of prohibited places was under-inclusive and failed to recognise that in the modern era, sensitive information may be held on sites which are not solely or primarily military ones. We also noted that the legislation does not currently protect sites which store sensitive economic information and which may be targeted by those whose aim is to injure the national interest.[91]

3.73 Provisional conclusion 4 stated:

> The list of prohibited places no longer accurately reflects the types of sites that are in need of protection. Do consultees agree?[92]

3.74 In addition, in the Consultation Paper we noted that the approach taken in the Serious Organised Crime and Police Act ("SOCPA") 2005, relating to "protected sites", involves designating sites. We suggested 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.

---

91 Consultation Paper, para 2.155.

92 Consultation Paper, para 2.161.

Such a list would be enacted in primary legislation, but would be capable of amendment by way of Statutory Instrument subject to the affirmative resolution procedure in Parliament. We did not, however, believe that this power should only apply to Crown or Royal land.

Consultation question 4

3.75 Consultation question 4 asked:

> 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?[93]

Consultation responses

3.76 Not many consultees engaged with either provisional conclusion 4 or consultation question 4. Those who did engage, such as the Bar Council and Criminal Bar Association, the Crown Prosecution Service and Peters and Peters, tended to agree.

3.77 Indeed, Peters and Peters asserted that the list of "prohibited places" in in the OSA 1911 is:

> … out of date and under-inclusive, omitting, for example, places such as data centres at which sensitive information is stored.[94]

3.78 The Open Rights Group submitted that sensitive sites were already adequately protected because they are included on the list of prohibited places scheduled to the SOCPA 2005.

3.79 While Peters and Peters considered that a common approach across the SOCPA 2005 and any new Official Secrets Acts legislation would "make sense", they emphasised concerns regarding the term "national security" and its potential to be manipulated if left undefined.[95]

3.80 In addition, the Trinity Mirror raised the concern that an unchecked power to create designated sites based on "national security" may create "a new criminal offence without a parliamentary debate" and potentially stifle "legitimate investigations in the public interest".[96]

3.81 In relation to provisional conclusion 4, Whistleblowers UK added:

---

93 Consultation Paper, para 2.163.

94 Peters and Peters, p 3.

95 Peters and Peters, p 4.

96 Trinity Mirror, by email.

In principle we agree, provided that the list does properly relate to national security and does not end up being widened to include, for example, council offices or schools.[97]

Analysis

3.82 The reason we included analysis of this issue in our Consultation Paper is because we did not consider that the existence of the provisions in the SOCPA 2005 was necessarily sufficient to deal with the potential problem of failing to include sites that should be prohibited places. As we noted in our Consultation Paper, there is inconsistency between the schemes for prohibited places listed in the OSA 1911 and the protected sites listed in the SOCPA 2005.[98] Some sites feature on one list but not the other, despite the provisions having similar purposes. We suggested that one consequence of this discrepancy is the potential for a site to be inadequately protected.

3.83 We agree with Whistleblowers UK that the list of prohibited places needs to retain a tight focus on the safety and interests of the state. This can partly be achieved through careful drafting of the regulation-making power. Another safeguard we believe is worth considering is a requirement, similar to the one contained in section 131 of the SOCPA 2005, for 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, by displaying notices on or near the site to which the order relates. This would ensure that an individual is given fair warning that he or she is approaching a location that is given enhanced protection by the criminal law.

3.84 The concerns raised by Peters and Peters and Trinity Mirror echo those raised by Whistleblowers UK in response to provisional conclusion 4. We believe that these concerns can be met through careful drafting of the provision that confers the power upon the Secretary of State and also by relying upon the affirmative resolution procedure for designation orders. This would mean that an order could not take effect unless voted upon by both Houses of Parliament. We would stress that we are not creating a new power: the power to designate a site as a prohibited place already exists under the OSA 1911.[99] What we are aiming to do is update the power to make it more effective, whilst taking the opportunity to introduce new safeguards such as increased Parliamentary scrutiny.

---

97 Whistleblowers UK, p 2.

98 Consultation Paper, para 2.158.

99 Section 3(c) and (d) Official Secrets Act 1911.

Recommendation 6.

3.85 The list of prohibited places should be drafted to reflect the modern espionage threat.

3.86 The Secretary of State should have the power, by statutory instrument subject to the affirmative resolution procedure, to amend the list of prohibited places where it is appropriate to do so in the interests of the safety or interests of the state.

3.87 The Secretary of State should be obliged to consider taking steps to inform the public of the effect of any designation order, including, in particular, by displaying notices on or near the site to which the order relates where appropriate.

Archaic language to be reformed and elements to be retained

3.88 The Official Secrets Acts 1911-1939 were enacted long before the digital age. They use language that is reflective of the era in which they were drafted. The provisions are verbose in places and the terms which are used are not reflective of the modern world. In our Consultation Paper, we noted that the legislation may not accurately reflect the type of information that requires protection in the modern age.[100] Using more generic terms to replace the references currently in the legislation to "secret official code word, pass word, sketch, plan, model and note" would, we provisionally suggested, ensure it achieves its stated aim and would prevent it from becoming out of date.[101] This was not a change of substance, since the legislation already makes reference to "other documents or information". For this reason, we did not believe that this change would increase the scope of the offences.

3.89 All the offences in the Official Secrets Acts 1911-1939, unlike the offences in the Official Secrets Act 1989, can be committed by anyone. The offences are not limited to Crown servants, government contractors or notified persons. We saw no reason why this ought to change. Currently, the offences encompass someone who obtains, collects, records, 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. Again, we saw no reason why this general application to any person ought to change.

Provisional conclusion 2

3.90 Provisional conclusion 2 therefore asked whether consultees agreed with the following three statements:

> Any redrafted offence ought to have the following features:

---

100 Consultation Paper para 2.166.

101 Consultation Paper para 2.167.

(1) Like the overwhelming majority of criminal offences, there should 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; and

(3) The offence should use the generic term "information" instead of the more specific terms currently relied on in the Act.[102]

Provisional conclusion 5

3.91 Provisional conclusion 5 stated:

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

Provisional conclusion 6

3.92 Provisional conclusion 6 stated:

> 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?

Consultation responses

3.93 Consultees who agreed with provisional conclusion 2 included News Group Newspapers, the Crown Prosecution Service and the Bar Council and Criminal Bar Association.

3.94 Peters and Peters generally agreed with provisional conclusion 2, but described paragraph (2) as "more controversial". They observed that merely obtaining non-public information without then passing it on, publishing it or using it for any further purpose is arguably not espionage as the general public would understand it.[103]

3.95 Those who disagreed, included Liberty, Guardian News and Media, the News Media Association and the National Union of Journalists. They objected to the introduction of "gathering" in paragraph (2) and/or to replacing the specific terms (for example, sketches, plans and models) with the generic term "information". It was argued that these changes, along with the retention of "obtains, collects, records, or publishes" would have a disproportionate effect on journalism.

3.96 For example, the National Union of Journalists submitted that:

---

[102] Consultation Paper, para 2.123.

[103] Peters and Peters, p 2.

> Journalists who obtain or gather information (including information about prohibited places) for the purposes of journalistic activity should not be committing an espionage offence.[104]

3.97 In addition, Guardian News and Media observed that new terms such as "possesses" and "gathers" were not defined, but "appear to widen the scope of the offences to someone who holds such information, even if they do not publish it". They added:

> This thus has the potential to severely impact on the role of journalists to *receive* as well as to impart information… As a point of principle (irrespective of whether they publish) journalists who receive, gather or obtain information of the sort covered by OSA 1911, including about prohibited places, should not be under the threat of prosecution, if there is a legitimate public interest in their possession of such information, even if it is not published.[105]

3.98 The responses to provisional conclusion 6 largely mirrored those to provisional conclusion 5. The Institute of Employment Rights argued that "modern legislation is required to reflect the digital age and incorporate modern developments in the area of security and intelligence".[106] News Group Newspapers, the Crown Prosecution Service, the Bar Council and Criminal Bar Association, and Peters and Peters agreed with both provisional conclusions 5 and 6. The Crown Prosecution Service gave an example of a case where the item obtained by a defendant – a "cryptography device" – did not fall easily into the language of the OSA 1911.[107]

3.99 While Guardian News and Media expressed strong opposition to provisional conclusion 2, it observed that modernising the language to remove anachronistic terms like "code words" and "replacing them with language that will future proof the legislation" was a positive step forward.[108]

3.100 The Government Response agreed that the current language was archaic but considered that our proposal to replace all the existing terms with "information" could cause problems for prosecutors. Their suggestion was to use "document, information or other thing", which would mirror the language in the Official Secrets Act 1989.[109]

Analysis

3.101 It was not our intention to broaden the scope of the offences in the OSA 1911 to make it easier to prosecute journalists. The legislation already refers to "any secret official code word, or pass word, or any sketch, plan, model, article, or note, *or other document or information*". Given that the legislation already uses the broad term "information", the things which precede it seemed to us to be redundant. For this

---

104 National Union of Journalists, p 2.

105 Guardian News and Media, pp 42 to 43.

106 Institute of Employment Rights, p 16.

107 Crown Prosecution Service, p 3. See G Corera, *Sailor Edward Devenney's fruitless attempt at betrayal* (12 December 2012), available at https://www.bbc.co.uk/news/uk-20701842.

108 Guardian News and Media, p 41.

109 Government Response, p 3.

reason, we did not consider that placing exclusive reliance upon this term would constitute a change of substance.

3.102 In relation to our proposed use of the term “gathers”, the legislation currently refers to an individual who obtains, collects, records, publishes or communicates something that is listed in the subsection. When we used the term “gathers” we did not intend for it to broaden the scope of the offences and simply used it as a synonym for some of the forms of conduct that are already encompassed by the legislation. For example, the legislation currently uses the term “to collect”. According to the Oxford English Dictionary this means, “to gather together into one place or group; to gather, to get together”. For this reason, we do not agree that relying upon the term “gather” would constitute an extension of the offences. For the avoidance of doubt, however, we have nevertheless removed the refence to “gathers” from our recommendation.

3.103 The analysis in our Consultation Paper was simply reflective of how the offences are currently drafted. We appreciate that the term “to publish”, which is currently used in the legislation, relates directly to journalism. This could be removed. Given the nature of espionage, however, the offence would still need to encompass those who communicate something listed in the subsection. This term is broad enough to include those who publish information. Such a change might be valuable in terms of clarifying the forms of conduct at which the legislation is aimed.

3.104 We appreciate the point made by the Crown Prosecution Service that the list of things encompassed by the offence may not, despite its breadth, encompass everything that might be targeted. The formulation provided in the Government Response does not appear to widen the scope of the offence and, by including the generic term “or other thing”, ensures that items such as memory sticks are encompassed by the offence. For the avoidance of doubt, as we stated in our Consultation Paper, we also believe that it is important that the term “information” is defined to include any program or data held in electronic form. This is the same terminology as is used in modern legislation such as section 8(1)(b) of the Fraud Act 2006.

3.105 There seems to us no reason why the Official Secrets Acts 1911-1939 should not continue to apply to everyone over whom the English courts have jurisdiction under those Acts (which means the jurisdiction is not limited to those physically in the UK). This will mean that they apply to all people in the UK, just like many other criminal offences generally (with the notable exception in this context of those offences in the Official Secrets Act 1989 which can only be committed by Crown servants, government contractors and notified persons).

Recommendation 7.

3.106 There should continue to be no restriction on who can commit the offences contained in the Official Secrets Act 1911 or in any replacement legislation.

3.107 There should continue to be separate offences of espionage by trespass and espionage by collection or communication of information.

3.108 The espionage by trespass offence should also continue to apply to those who approach, inspect, pass over or enter any prohibited place within the meaning of the Act.

3.109 The collection and communication offence should continue to be capable of being committed not only by someone who communicates information, but also by someone who obtains it.

3.110 References in the Official Secrets Acts 1911 and 1920 to a sketch, plan, model, note and secret official pass word and code word are anachronistic and should be replaced with "document, information or other article". Information should be defined to include any program or data held in electronic form.

Reverse burdens of proof

3.111 Section 1(2) of the OSA 1911 provides that the prosecution does not need to show that the defendant carried out 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 their "known character as proved", it *appears* that he or she possessed a purpose prejudicial to the safety or interests of the state. Further, subsection (2) also provides that any sketch, plan, document, or information etc that is obtained, made, communicated etc shall be deemed to have been so for a purpose prejudicial to the safety or interests of the State, unless the contrary is proved. We suggested in our Consultation Paper that this was objectionable as it appeared to introduce a standard of proof less than the criminal standard of beyond reasonable doubt.[110]

3.112 Section 2(1) of the Official Secrets Act 1920 ("OSA 1920") provides that communication with a foreign agent shall be evidence of the commission of the offences in section 1 of the OSA 1911. In addition, section 2(2) of the OSA 1920 provides that a person shall, unless he or she proves the contrary, be deemed to have been in communication with a foreign agent if he or she has visited the address of a foreign agent, or the name and address of – or any other information regarding – a foreign agent has been found in his or her possession, has been supplied to him or her, or has been obtained by him or her from another person.

[110] Consultation Paper para 2.177.

3.113 On the face of it, section 2(2) imposes a reverse burden of proof on the defendant. Rather than requiring the prosecution to prove the case against the defendant, it requires the defendant to disprove the case against them. As we explained in our Consultation Paper, reverse burdens of proof are only compatible with the presumption of innocence guaranteed by Article 6 of the ECHR under certain circumstances.[111]

3.114 To ensure an interpretation that is compatible with the ECHR, we stated in our Consultation Paper that a court would most be most likely to invoke section 3 of the Human Rights Act 1998 to "read down" this provision so that it imposed only an evidential burden on the defendant to adduce sufficient evidence to raise the question of whether he or she had been in communication with a foreign agent as an issue. 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. We considered that the courts would take a similar approach to section 1(2) of the OSA 1911.

3.115 Furthermore, it is generally accepted that deeming provisions such as those found in section 1(2) of the OSA 1911 and section 2(2) of the OSA 1920 have no place in the criminal law.[112] Whilst we acknowledged the difficulty in proving the commission of espionage offences, we argued that it was preferable for the legislation not to contain provisions such as these.

Consultation question 5

3.116 Consultation question 5 asked:

> 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?[113]

Consultation responses

3.117 Consultees, including the Bar Council and Criminal Bar Association, Peters and Peters and the Crown Prosecution Service, were in favour of removing these provisions from the Official Secrets Acts 1911 and 1920. The Crown Prosecution Service stated that they did not believe they had ever used these provisions in practice. The Government Response was also in favour of removing the provisions.

Analysis

3.118 The responses we received to this consultation question confirm our initial view that these provisions are redundant and fulfil no useful purpose. In addition, as a matter of

---

111 For a more detailed examination of Article 6 of the European Convention on Human Rights and reverse burdens of proof, see paras 2.180 – 2.189 of the CP.

112 See, eg P Alldridge, "Some Uses of Legal Fictions in Criminal Law", in W Twining and M Del Mar (eds) *Legal Fictions in Theory and Practice* (2015) at pp 367 – 384.

113 Consultation Paper, para 2.190.

principle, provisions which dilute the burden of proof borne by the prosecution should be employed sparingly in the criminal law.

Recommendation 8.

3.119 We recommend that sections 1(2) of the Official Secrets Act 1911 and section 2(2) of the Official Secrets Act 1920 should be repealed.

Redundant provisions

3.120 In our Consultation Paper we noted that a number of provisions in the Official Secrets Acts 1911 and 1920 appear to be little used in the modern era. For example, section 7 of the OSA 1911 creates a number of offences connected with harbouring spies.[114] Section 1 of the OSA 1920 creates a number of offences relating to the unauthorised use of uniforms, falsification of reports, forgery, personation, and false documents.[115]

3.121 As discussed above, section 2(1) of the OSA 1920 provides that communication with a foreign agent shall be evidence of the commission of the offences in section 1 of the OSA 1911. We agree that communication with a foreign agent may be relevant to the question of whether a defendant has committed an espionage offence, but consider it is best dealt with as circumstantial evidence admissible in accordance with the normal rules of evidence.

3.122 Under section 3 of the OSA 1920, it is an offence to interfere with officers or members of Her Majesty's forces in the vicinity of a prohibited place. Section 3 provides:

> 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.

3.123 This conduct is likely also to amount to an attempt under section 7 of the OSA 1920 and/or aggravated trespass contrary to section 68 of the Criminal Justice and Public Order Act 1994.

3.124 Section 6 of the OSA 1920 creates a mechanism for the police to apply for the power to require an individual to give information relating to an offence or suspected offence, or to require that individual to attend a place specified by the police officer. An individual who fails to comply with the request for information, or to attend the specified place, commits a criminal offence. Section 6 provides:

> (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

---

114 Consultation Paper, paras 2.59 to 2.61.

115 Consultation Paper, paras 2.78 to 2.84.

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.

3.125 Section 7 of the OSA 1920 criminalises acts preparatory to the commission of an offence under the Official Secrets Acts. It also makes it an offence for any person to solicit, incite or endeavour to persuade another person to commit an espionage offence, or to aid or abet the commission of an espionage offence. Section 7 provides:

> 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.

3.126 The preparatory offence contained in section 7 of the OSA 1920 encompasses conduct that would not fall within the scope of a criminal attempt under the Criminal Attempts Act 1981.[116] The conduct element of the offence contained in section 7 includes "doing an act preparatory" to an espionage offence whereas the conduct element of the offence contained in the Criminal Attempts Act 1981 ("CAA 1981") is "doing an act *more than merely* preparatory". Thus, the offence contrary to section 7 of the OSA 1920 criminalises conduct at an earlier stage than the general law of

---

[116] It was determined in the Court of Appeal that the word "and" in "abets *and* does an act preparatory" is instead to be read as "or": *R v Oakes* [1959] 2 QB 350, [1959] 2 All ER 92. See also *R v Bingham* [1973] QB 870, [1973] 2 All ER 89.

attempt. Furthermore, following the Court of Appeal's decision in *R v Pace*,[117] the prosecution must prove intention as to every element of the substantive offence that the defendant attempted to commit under the CAA 1981. This does not appear to be necessary under section 7 of the OSA 1920. The remainder of the offences under section 7 of the OSA 1920 are duplicated by other statutes.[118]

Consultation responses

3.127 We did not ask a specific question directed to these provisions, but we did receive comments on them from a number of consultees. For example, the News Media Association considered that section 6 of the OSA 1920 had a chilling effect on freedom of expression.[119] The Government Response stated that section 6 of the OSA 1920 ought to be repealed.

Analysis

3.128 We agree that section 6 of the OSA 1920 is anomalous and that it ought to be repealed.

3.129 We did not consult specifically on whether the preparatory offence (doing an act preparatory to the commission of an offence) under section 7 of the OSA 1920 should be retained, and so make no recommendation as to that offence. However, we note that the remainder of section 7 appears no longer to serve a useful function, given that it overlaps with the law of attempts, secondary liability, and the inchoate offences contained in Part 2 of the Serious Crime Act 2007.[120] For this reason, we believe that those other elements of section 7 ought to be repealed. This would bring the offences contained in the OSA 1911 in line with other criminal offences. Finally, the continued existence of the offence of harbouring spies in section 7 of the OSA 1911 appears to be anomalous given the existence of the offence of assisting an offender in section 4 of the Criminal Law Act 1967. Once again, legislative developments which have taken place since the enactment of the Official Secrets Acts 1911-1939 have superseded and made redundant this specific offence.

Recommendation 9.

3.130 We recommend that section 7 of the Official Secrets Act 1911 and section 2(1) and section 6 of the Official Secrets Act 1920 should be repealed without replacement.

3.131 The offence of doing an act preparatory to espionage should be retained. Save for that, section 7 of the Official Secrets Act 1920 should be repealed.

---

117 [2014] EWCA Crim 186; [2014] 1 WLR 2867.

118 Part 2 of the Serious Crime Act 2007 and the Accessories and Abettors Act 1861.

119 News Media Association, p 18.

120 Under section 44 of the Serious Crime Act 2007, a person commits an offence if (a) he does an act capable of encouraging or assisting the commission of an offence; and (b) he intends to encourage or assist its commission.

Extraterritoriality

3.132 Section 10 of the OSA 1911 provides that the offences contained in that Act can be committed by a British Officer (currently undefined, but likely to mean Crown servant) or subject outside the United Kingdom. A person who is not a British Officer or subject commits no offence if they engage in conduct prohibited by the OSA 1911 abroad.

3.133 Section 10 of the OSA 1911 provides as follows:

> (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 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.

3.134 In the Consultation Paper, we provisionally concluded that the territorial ambit of the OSA 1911 is insufficient to offer adequate protection to sensitive assets abroad and asked consultees whether they agreed. We suggested that it should not matter whether the individual in question, for example a contractor abroad, is a British Officer or subject, provided he or she engages in the conduct caught by the offence with the requisite fault element.

Provisional conclusion 7

3.135 Provisional conclusion 7 stated:

> 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?[121]

Consultation responses

3.136 The Crown Prosecution Service agreed with this provisional conclusion. The Bar Council and Criminal Bar Association agreed in principle, but thought there needed to be more detail provided in order to evaluate it properly. Other consultees, including the Open Rights Group, questioned the practicability of the provisional conclusion and, in particular, whether a foreign country would be likely to extradite one of its citizens to the United Kingdom to face trial. The National Union of Journalists and the News Media Association both disagreed on the grounds that it could lead to more prosecutions of journalists.

3.137 The Government Response agreed with the provisional proposal in the Consultation Paper, stating:

---

[121] Consultation Paper, para 2.175.

> We favour expanding [the territorial ambit] so that the offences can be committed overseas (i) by any British citizen or resident and (ii) by any other person where there is a sufficient link to the UK. We favour defining such a link to include cases (i) where the espionage is carried out remotely by attacking computer servers, computers or other electronic equipment sited in the UK or on which UK-related information is being held, processed or transmitted (regardless of whether the computers etc. are in public or private ownership), and (ii) where the information is held in a UK embassy or other diplomatic mission or is in the possession of HMG outside a mission.[122]

Classified evidence

3.138 As part of our request for further evidence, we have seen evidence relating to extra-territorial conduct. This has assisted in our analysis of the 'link' that ought to exist between the individual's behaviour and the interests of the United Kingdom. The evidence cannot be published owing to its security classification, but the following three hypothetical examples illustrate the risks revealed by the classified evidence:

(1) A is working for a government-sponsored group in a foreign state. A is a national of this foreign state. While within the foreign state, A steals Defence Science and Technology Laboratory (DSTL) information relating to proprietary military technology held on servers in Yorkshire in support of their own country's military technology programme.

(2) B is a national of an allied state, working for a company contracted by a foreign state. While within the foreign state, B targets government HR information held on servers in another allied state to identify targets for blackmail or recruitment.

(3) C is a Crown Servant attached to an embassy within a neutral state. An intelligence officer working for a third, foreign, state covertly accesses and copies sensitive documents held by C.

Analysis

3.139 We used the phrase "significant link" when we introduced the concept at paragraphs 2.172 to 2.173 of our Consultation Paper. The phrase "sufficient link" was, however, used in provisional conclusion 7.[123] That was a mistake; it was our intention to use the phrase "significant link". "Significant link" implies a higher test, and echoes the changes made to the Computer Misuse Act 1990 by the Serious Crime Act 2015. This was the concept we relied upon in our Consultation Paper.

3.140 Section 5 of the Computer Misuse Act 1990 defines "significant link" in various ways. For example, the offence contrary to section 3ZA of the Computer Misuse Act 1990 (committing an unauthorised act causing, or creating a risk of, serious damage of a material kind) can be committed anywhere in the world and by any person provided the damage that is caused or risked occurring within the United Kingdom. The defendant's nationality is immaterial. In our Consultation Paper we were not

---

122 Government Response, p 7.

123 Consultation Paper, para 2.175.

suggesting that this definition be incorporated wholesale, but it was intended to provide an illustration of how the territorial ambit of an offence can be expanded.

3.141 However, it is noteworthy that the Computer Misuse Act 1990 and a reformed espionage offence could, in certain circumstances, criminalise variously acts that are fundamentally similar (ie illegally obtaining or communicating information owned by the UK government, coupled with purpose/intention). Whether it is prosecuted as a Computer Misuse Act offence or espionage could come down to a somewhat technical distinction as to whether the computer used to access the information was located within a UK-owned site. The evidence that we have seen is particularly telling in this regard (see (1) and (2) above): many acts of 'espionage' against UK data/information are carried out using computers.

3.142 We have not consulted on reform of the Computer Misuse Act, and so make no recommendations on its reform in light of any new espionage offence. However, we see force in an argument that the two offences should be aligned to ensure that offending behaviour, especially where the defendant has a purpose prejudicial to the state, is criminalised appropriately.

3.143 One particular matter raised in the evidence, as illustrated in the hypothetical example at 3.138(2), and echoed in the Government Response (at 3.137), is the nature of the threat to UK proprietary data. The technical reality of modern data sharing and storage, as well as engagement with the private sector, means that UK proprietary data (ie data owned or controlled by the UK government) can be held on servers outside the jurisdiction. The threat facing this data is no different to the threat facing data held within the UK – it can be targeted in precisely the same way – and the damage resulting from its targeting can be just as severe. Indeed, what matters in determining the potential for damage is not simply whether the data is held on a server within the jurisdiction or whether the UK happens to own the server; the damage attends to the data itself. This data should be afforded the same protection as data held on servers in the UK. The extraterritoriality provisions in any new espionage offence should reflect the modern reality of data storage, and therefore "significant link" should be defined to include UK proprietary data. Given the nature of modern espionage, failing to define "significant link" in such a way would weaken the effect of many of our other recommended reforms to espionage legislation.

3.144 We acknowledge the point made by the Open Rights Group about the difficulty in prosecuting some cases where the defendant is overseas. This is an issue that applies with greater force to offences that currently exists, such as those contained in the Computer Misuse Act 1990. For example, an individual commits an offence contrary to section 3ZA of the Computer Misuse Act 1990 even though he or she may have been outside the United Kingdom, provided that his or her unauthorised act was done in relation to a computer situated in the United Kingdom. This difficulty did not impede the extension of the territorial ambit of those offences when they were expanded in 2015.

3.145 We appreciate that our Consultation Paper may not have described with sufficient detail what forms of conduct we envisaged being encompassed by a modified version of the OSA 1911.

Example

3.146 N is a British citizen employed at the British embassy in Ruritania. N uses his access to sensitive areas of the embassy to carry out reconnaissance on behalf of a foreign government. N has committed an offence under section 1 of the OSA 1911.

3.147 L is a member of local staff at the British embassy in Ruritania. L uses her access to sensitive areas of the embassy to carry out reconnaissance on behalf of a foreign government. Because L is not a British officer or subject she has committed no offence under the OSA 1911.

3.148 Our aim in the Consultation Paper was to ensure that, in the example above, the local staff member commits an offence despite the fact he or she is not a British Officer or subject. The term "significant link" ought to be defined to ensure that it encompasses those who have access to British assets located outside the United Kingdom and which may be targeted for the purposes of espionage.

3.149 We appreciate the concerns expressed by, amongst others, the News Media Association and the National Union of Journalists, about the impact that extending the territorial ambit of the offences might have on journalists. It is worth recalling that a journalist would only commit an offence if he or she possessed the requisite culpable state of mind – acting with the purpose prejudicial to the safety or interests of the state – which would, under our recommendations, be narrowed to require proof of subjective fault.

Recommendation 10.

3.150 The territorial ambit of the offences contained in the Official Secrets Acts 1911-1939 should be expanded so that they can be committed irrespective of the individual's nationality. The test should be whether there is a "significant link" between the individual's behaviour and the interests of the United Kingdom.

3.151 "Significant link" should be defined to include not only the case where the defendant is a Crown employee or contractor, but also the case where the conduct relates to a site or data owned or controlled by the UK government (irrespective of the identity of the defendant).

3.152 To ensure that sensitive UK assets overseas receive maximum protection, any new definition of "prohibited place" (see recommendation 6) should explicitly provide that such places may be overseas.

Current offence	Recommended offence (relevant changes in *italics*)
Forms of conduct (section 1(1))	
(a) "approaches, inspects, passes over or is in the neighbourhood of, or enters any prohibited place within the meaning of the Act;"	[No change] Approaches, inspects, passes over or is in the neighbourhood of, or enters any prohibited place within the meaning of the Act;
(b) "makes any sketch, plan, model, or note…; or"	*Collects or records any document, information or other article…*
(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…"	*Communicates or publishes any document, information or other article…*
Useful to an "enemy" (section 1(1)(b)-(c))	
(b) "makes any sketch… calculated to be or [objectively] might be or is intended to be directly or indirectly useful to an enemy; or"	Collects or records… calculated to be or [objectively] might be or is intended to be directly or indirectly useful to a *foreign power*
(c) "obtains, collects… information calculated to be or [objectively] might be or is intended to be directly or indirectly useful to an enemy."	Collects or records… calculated to be or [objectively] might be or is intended to be directly or indirectly useful to a *foreign power*
Purpose prejudicial (section 1(1))	
D committed any of 1(1)(a)-(c) above for a: - "purpose" [subjectively determined] - that was "prejudicial to the safety or interests of the State" [objectively determined]	D committed any of 1(1)(a)-(c) – or their reformed equivalents – *for a purpose he or she knew or had reasonable cause to believe was prejudicial to the safety or interests of the State.*
Extraterritoriality (section 10(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."	The offences should be capable of being committed *irrespective of the individual's nationality*, so long as there is a *significant link between the individual's behaviour and the interests of the United Kingdom*.

PART II

Unauthorised Disclosures

Chapter 4: The Official Secrets Act 1989 and the requirement to prove damage

INTRODUCTION

4.1 Chapter 3 of our Consultation Paper examined the Official Secrets Act 1989 ("OSA 1989"), evaluated the extent to which the Act is in need of reform, and sought consultees' views on a number of options.[124] In this Chapter, we briefly restate the current law before considering in more detail the requirement to prove that a disclosure is damaging.

4.2 In our Consultation Paper, we provisionally proposed that the requirement to prove damage should be replaced in some of the offences in the OSA 1989 with more stringent fault elements. We set out this proposal as part of what we considered a balanced range of reforms. Our re-structuring was designed to address perceived weaknesses in the offences while guarding against over-criminalisation. As we discuss below, our proposals were rejected by the majority of consultees. One of the overriding concerns expressed by consultees was that, absent any public interest defence, the damage requirement acted as a proxy for such a defence. Further concern was expressed that we had not received evidence to support our conclusion that the damage requirement had the potential to limit prosecutions that would otherwise be in the public interest.

4.3 In this Chapter we examine and analyse consultees' responses to our other reform proposals before making a series of recommendations. It remains our view that – for OSA 1989 offences *other than the sections 5 and 6 offences* (to which journalists would be subject) – the requirement to prove damage should be removed. The public interest disclosure regime that we recommend in the third part of this report is designed to protect disclosures in the public interest, and does so in a more structured and direct way than a damage requirement (which protects public interest disclosures only indirectly and imperfectly). The regime we propose is also designed to ensure that prosecutions are not unjustly hampered by the need to disclose further secret material in open court. We remain of the view that this remains a real risk with the damage requirement – whether or not there was evidence of this having been a problem in the past – and our assessment of the evidence supports our position.

THE BACKGROUND TO THE OFFICIAL SECRETS ACT 1989

4.4 Before examining the problems which we identified with the OSA 1989, it is worth describing the background that led to its enactment. Prior to its repeal by the OSA 1989, section 2 of the Official Secrets Act 1911 ("OSA 1911") criminalised the unauthorised disclosure of *all* official information entrusted to Crown servants. Section 2 of the OSA 1911 was described in 1972 by the Franks Committee as a "legislative mess".[125] The Franks Committee concluded that section 2 was drafted in very wide

---

124 We summarise the law in our Consultation Paper, paras 3.21 to 3.133.

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

terms and was highly condensed. On one calculation, section 2 permitted two thousand differently worded charges to be brought under it.[126] The Franks Committee concluded that section 2 of the OSA 1911 needed to be replaced with a more narrowly drawn provision.

4.5 The Government did not succeed in implementing the Franks Committee's recommendation until after the publication of a White Paper in 1988. In that paper, the Government outlined its aims 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 as an oppressive instrument for the suppression of harmless and legitimate discussion. Because section 2 goes so much wider than what is necessary to safeguard the public interest, its necessary role in inhibiting harmful disclosures is obscured.[127]

4.6 The aim in 1988 in reforming the law was therefore to enact a narrower offence than that contained in section 2 of the 1911 Act. The OSA 1989, which repealed section 2 of the 1911 Act, achieves this aim by specifying that it only applies to certain categories of information: information relating to security or intelligence; defence; international relations; crime and special investigation powers; and information entrusted in confidence to other states or international organisations. The offences, apart from those in sections 5, 6 and 8(4), can only be committed by Crown servants or government contractors. Unusually, these are not offences which can be committed simply by anyone within the territorial jurisdiction.

THE REQUIREMENT TO PROVE DAMAGE

4.7 As discussed in our Consultation Paper, many of the offences in the OSA 1989 have a damage requirement. The prosecution must prove that the defendant's unauthorised disclosure caused damage, or was likely to cause damage, to a specified state interest (such as defence).[128]

4.8 Each of those sections which has a damage requirement defines damage in a specific way. For example, section 2(2) of the OSA 1989 states that an unauthorised disclosure of any information, document or article relating to defence 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

---

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

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

128 Consultation Paper, para 3.137.

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 these effects.

Defences

4.9 For each of those offences with a damage requirement, there is a corresponding defence of "not knowing and having no reasonable cause to believe" that the disclosure would be damaging.[129] To return to the example used above, section 2(3) of the OSA 1989 provides:

> 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 or 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.

4.10 On the face of it, these defences place the legal burden of proof on the defendant. This means that it would be for the defendant to prove that he or she did not know or had no reasonable cause to believe that the information, document or article related to defence, or that its disclosure would be damaging. The failure to discharge this burden would, assuming the prosecution established the other elements of the offence, result in conviction.

4.11 In *R v Keogh*,[130] however, the Court of Appeal invoked section 3 of the Human Rights Act 1998 to interpret the burden as being an evidential one (see also our discussion at 3.113). As such, providing the defendant can adduce *some* evidence that he or she lacked reasonable cause to believe the unauthorised disclosure was damaging, then the prosecution must prove beyond reasonable doubt that the defendant had reasonable cause to believe so. Reasonable cause to believe has been interpreted as an objective test.[131] The editors of *Blackstone's Criminal Practice* suggest:

> For offences requiring damaging disclosure, it is necessary for the prosecution to prove not only that the disclosure is damaging but also that the person making the disclosure knows or has grounds to believe that it would be damaging (in the sense that it is likely to have that effect). It is insufficient for the prosecution to prove that there were reasonable grounds to believe that the disclosure might be damaging or that this was merely a possibility.[132]

---

129 Arguably this is a denial of fault element rather than a defence.

130 [2007] EWCA Crim 528; [2007] 1 WLR 1500.

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

132 *Blackstone's Criminal Practice* (2020) at para B9.45.

The requirement to prove *any* damage

4.12 In our Consultation Paper we stated that the requirement to prove *any* damage was in some cases problematic:

> 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.[133]

4.13 There are two points here, one of principle and the other practical. First, the culpability of an official making an unauthorised disclosure may be identical, whether or not that disclosure was in fact damaging. For example, an official to whom the Act applies might make an unauthorised disclosure of information in the belief that it reveals the location of special forces based overseas, but which is in fact harmless (perhaps because it is wrong, outdated, or has been deliberately planted to test their willingness to commit a criminal offence). It is not obvious why such an official is in principle less culpable than they would be if the disclosure of the information happened to be harmful. Provided the defendant possessed the requisite state of mind, conduct such as this would amount to an attempt.[134] It is worth emphasising again that the offences in question only apply to Crown servants and contractors. This is not an offence that could apply to citizens generally. The concerns about over-criminalising conduct that is not causing damage are quite different. Crown servants ought not to be making unauthorised disclosures with awareness that they are likely to damage one of the specified interests (such as defence) when one of their responsibilities as a Crown servant is to act for the good of the state.

4.14 The second point is a practical one. During our pre-consultation engagement – and this has been confirmed in evidence we have seen – we heard from stakeholders representing a number of Government departments that the requirement to prove damage or likelihood of damage can make it difficult to bring a prosecution. We were told that in some cases proving that damage was caused or likely to be caused will not only require the prosecution to disclose further highly sensitive information but also to reveal the existence of vulnerabilities to, for example, defence capabilities. We were told by these stakeholders that the requirement to place such information before a jury had, on occasions in the past, precluded prosecutions being brought.

4.15 In our Consultation Paper,[135] we suggested that shifting to a model of offence that was not based on results (damage) but on the culpable state of mind of the person who disclosed the information could provide an answer to this problem. As we explained in

---

133 Consultation Paper, para 3.146. Emphasis in original.

134 It is worth noting that under the present law, someone assisting that person – eg a journalist in knowing receipt – would be guilty of aiding and abetting the offence; a person who encouraged the unauthorised disclosure could be prosecuted under Part 2 of the Serious Crime Act 2007, irrespective of whether the disclosure was made.

135 Consultation Paper, paras 3.153 to 3.163.

our Consultation Paper, this is a method of drafting which criminalises conduct rather than results. An example would be the offence of fraud, which is contained in the Fraud Act 2006. Section 2 of the Fraud Act 2006 criminalises an individual who dishonestly makes a false representation with the intention of making a gain or causing a loss or exposing another to a risk of loss. The fact that no one was deceived by the false representation is irrelevant to the defendant's criminal liability, as is the fact that no loss may actually have been caused.

4.16 With these points in mind, provisional conclusions 9 and 10 and consultation question 6 were designed to seek consultees' views on whether and how to reform the requirement to prove damage. We examine consultees' responses below.

4.17 As will be seen from the consultation responses set out below, many consultees were not persuaded that it was necessary or desirable to reform the law in the way we suggested. We understand and accept the difficulty that stakeholders faced in evaluating our analysis of this issue, given the lack of publicly available information about prosecutions under the OSA 1989 which have *not* been brought. We will return to this point below.

4.18 It is also worth noting at this point that many consultees, especially those representing the media, focused on the relationship between damage and the offences contained in sections 5 and 6 of the OSA 1989. This is unsurprising given that these are the offences that can be committed by non-Crown servants, including journalists. For the avoidance of doubt, we were not proposing any amendment to the damage requirement of these provisions. We therefore are not recommending any changes to them in this Report. For individuals who are not Crown servants or government contractors, the prosecution would therefore still have to prove damage. On reflection, and in view of the confusion, it is clear that this point ought to have been made more explicit in the consultation question.

Provisional conclusion 9

4.19 Provisional conclusion 9 stated:

> We provisionally conclude that, as a matter of principle, it is undesirable for those who have disclosed information contrary to the OSA 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?[136]

4.20 The Crown Prosecution Service agreed with the provisional conclusion, stating:

> The conduct of the prosecution of a person who has disclosed information etc. which is damaging to national security to others may itself cause further damage to the need to protect that information if it is conducted, as it ought normally to be, in open court. If appropriate safeguards are not available to protect the information, the prosecution may have to be stopped because the importance of the public interest in protecting the information outweighs the importance of the public interest in bringing

[136] Consultation Paper, para 3.137.

the person who unlawfully disclosed it to justice. In so doing, the latter important public interest is thus frustrated.

So, yes, we agree, it is undesirable for us not to be able to proceed with an OSA offence because measures to safeguard the information in the criminal process are not available. The intelligence community in this country or another, for instance, will be made aware of the fact of the breach so that they can take appropriate steps in respect of it, but if they fear further damage being caused by the criminal process (which includes the circle of knowledge being expanded even within reasonable bounds to advocates, jury, court officials etc.) then the case will not be able to proceed without appropriate safeguards in place to assure them of the control which will be exercised over the information.

Risk management is therefore key, i.e. assessing risks including the importance of the information and who may come to learn of it, the likelihood of those risks being realised, the safeguards available in principle, and again the likelihood of securing them. A not dissimilar principle occurred, by way of illustration, in *Incedal* [2016] EWCA Crim 11, i.e. the critical importance of hearing some of the trial *in camera*.[137]

4.21 Peters and Peters also agreed with the provisional conclusion and noted that:

> … previous attempts have been made to address this problem both through procedural measures such as the possibility of conducting hearings in private and the substantive provisions in the 1989 Act which give the prosecution the option of proving not that the disclosure in fact caused damage, but that the information in question fell within a certain class and that disclosure of information of that class was likely to cause the required damage. However, as discussed by the Commission, stakeholders report that these measures have been unsuccessful and that the damage element of the offences can still pose an insurmountable hurdle to bringing a prosecution. We accept this viewpoint and agree that it is unsatisfactory that those who have committed a disclosure offence can evade criminal liability for this reason.[138]

4.22 Other consultees, particularly those representing the media and non-governmental organisations, responded to this provisional conclusion with views ranging from scepticism to strong opposition. We examine their arguments below.

Insufficient evidence to support a change in the law

4.23 In their joint response, the Bar Council and Criminal Bar Association agreed in principle with the provisional conclusion, but queried the evidence on which it was based:

> …the Law Commission is presumably privy to empirical evidence rather than simple assertion. How many prosecutions, which otherwise would have been brought, have been abandoned for this reason as opposed to the inherent sensitivity of the information?

---

137 Crown Prosecution Service, by email 8 June 2012.

138 Peters and Peters, p 6.

> We feel it is important to emphasise that agreement with this principle does not lead inescapably to the conclusion that it is necessary to relieve the prosecutor of any burden of proving that conduct engaged in was of a type capable of causing damage.[139]

4.24 Liberty stated:

> …the Law Commission appears to adopt, without argument, the claim of unidentified "stakeholders" that disclosures must be criminalised regardless of the actual harm caused. Rather than examining the case for a real damages threshold, it offers only a choice between whether the offence would be committed where an individual knew, or merely believed, that the disclosure would be capable of causing damage. It also simply presumes that the meaning of the word, 'damage', would remain tied to the extremely loose definition in the 1989 Act. No other alternatives – beyond the Law Commission's later discussion, and rejection, of a public interest defence – are even considered.[140]

4.25 In their joint response, Campaign for Freedom of Information and Article 19 stated:

> If the Commission has been persuaded that… [the requirement to prove damage is an obstacle to prosecution], some account of the evidence it has seen would be expected: none is given. There is no indication that it has subjected what it has been told to critical examination. No example of any damaging disclosure which has gone unpunished is cited. No indication of the number of such cases is given.[141]

4.26 Professor Lorna Woods, Dr Lawrence McNamara and Dr Judith Townend stated that they were: "… not persuaded that the evidence or arguments presented in the consultation document justify removing this important protection".[142]

4.27 ITN submitted:

> The Consultation suggests proving damage has meant suspects have avoided criminal liability – but absolutely no evidence is given to back this suggestion. It is important if changes are made to this highly sensitive area of law the changes are based on evidence that justify reform - not broad, sweeping, unsubstantiated assertions.[143]

4.28 News Group Newspapers agreed with the general proposition but were sceptical as to how often the requirement to prove damage made it untenable to proceed with a prosecution.[144]

---

139 Bar Council and Criminal Bar Association, paras 37 to 38.

140 Liberty, para 32.

141 Campaign for Freedom of Information and Article 19, para 14.

142 L Woods, L McNamara and J Townend, para 2.10.

143 ITN, p 6.

144 News Group Newspapers, para 9.

Removal of an opportunity to consider public interest

4.29 Some consultees argued that the damage test acted as a quasi-public interest defence. For example, Guardian News and Media stated:

> The current damage requirement in the OSA 1989 has meant that, in effect, most of the OSA 1989 offences implicitly include an element of public interest.[145]

4.30 Similarly, the Courage Foundation stated:

> Removing the requirement to prove damage would be a retrograde step that takes us back towards the discredited 1911 Section 2 and its catch-all provisions. In principle, criminal sanction should only be applied to disclosures that can be demonstrated to have the potential to cause serious damage. The requirement to prove damage under the 1989 Act was explicitly stated to have a public interest component.[146]

Criminalising embarrassing, but not damaging, disclosures

4.31 Other consultees were concerned that remodelling the offence in the way we suggested risked criminalising disclosures that were merely embarrassing rather than harmful. For example, Dr Ashley Savage – an academic with expertise in the law relating to whistleblowing – agreed with our provisional conclusion, but cautioned that:

> …it would also be undesirable for public organisations to use the same justification to avoid disclosing potentially embarrassing information.[147]

4.32 Public Concern at Work stated:

> We are alarmed by the absence of any recognition in the report that removing the damage requirement risks lowering the bar for criminal prosecutions to include situations where a civil servant leaks information that merely embarrasses the Government rather than causes actual damage to national security.[148]

4.33 Similarly, Trinity Mirror stated:

> Although Trinity Mirror accepts that it would be undesirable for national security to be compromised in order to prove a damaging disclosure, it would be equally undesirable to prosecute on a matter that was not damaging to the State, but merely embarrassing or inconvenient, in the knowledge that damage would not have to be proved. Section 1(5) of the Act currently allows for a defence of lack of belief that a disclosure would be damaging. Trinity Mirror suggests that the requirement of damage should remain, subject to the use of Public Interest Immunity Certificates if appropriate and if National Security is at risk of being compromised.[149]

---

145 Guardian News and Media, p 59.

146 Courage Foundation, p 2.

147 Dr Ashley Savage, para 8.

148 Public Concern at Work, para 9.

149 Trinity Mirror, by email.

Effect on public interest journalism

4.34 As we pointed out above, our provisional conclusion was not intended to impact on the offences that can be committed by journalists or citizens generally; sections 1 to 4 apply only to Crown servants. Because we did not make this clear, consultees representing the media were rightly concerned about the impact this provisional conclusion would have on journalistic activity. For example, News Group Newspapers stated:

> Put shortly, if a journalist has published information the publication of which cannot be shown to be damaging to security and intelligence, defence or international relations, nor be shown to be likely to cause such damage, nor (in the case of security and intelligence information) shown to be information which falls within a class or description of information which would be likely to cause such damage then - regardless of the journalist's state of mind - the journalist should simply not be guilty of a criminal offence under the Official Secrets Act. For this reason, NGN believes that the offence should continue to require proof or likelihood of damage, as in the structure currently contained in section 5(3) of the OSA 1989.[150]

4.35 For the same reason, the National Union of Journalists stated:

> The NUJ strongly condemns the proposal to remove the requirement for prosecutors to prove that a disclosure was damaging. A requirement to prove damage must remain a prerequisite to establishing criminal liability in the area of unauthorised disclosures of information under the official secrets laws (or any successor). While we also oppose the recommendation to remove the damage requirement for primary disclosers, it is deeply disturbing that the Law Commission envisages a journalist could be prosecuted without any requirement for the authorities to prove that the disclosure caused damage. Anything short of a clear requirement to prove damage is likely to have a serious chilling effect on the exercise of public interest journalism. We urge the Law Commission to make it clear that there will be no recommendations or support for legal changes that would relax or abandon the requirement to prove damage before a journalist could be prosecuted.
>
> Section 5(3) of the 1989 Official Secrets Act provides an important safeguard for journalists and we implore the Law Commission to recommend its preservation. Removal of this safeguard would pose an existential threat to journalism focused on investigating national defence and security.
>
> Our concerns are in no way assuaged by the Law Commission's recommendations on the introduction of a requirement to prove subjective fault.[151]

4.36 Similarly, ITN stated:

> The proposals if implemented will mean criminalisation of disclosures that cause no harm and a far greater likelihood of the prosecution of editors, journalists and whistleblowers. It will inevitably have the effect of reducing the disclosure of

---

150 News Group Newspapers, para 9.

151 National Union of Journalists, p 17.

information the public should know about and what is reported through increased police powers over journalists.[152]

4.37 The BBC stated:

> If the harm test is removed from the current legislation, the result would be to open up again the scope of the offences which, in our view, would be an unjustifiable restraint on journalism and freedom of speech as protected under Article 10 of the European Convention on Human Rights ("ECHR"). If any new legislation contained a public interest defence (as discussed below), this effect would be mitigated. However, in the absence of a public interest defence we cannot support the Commission's conclusion.[153]

Managing the trial process to reduce the risks of proving damage

4.38 UK Open Government Network – part of the Open Government Partnership, an international initiative campaigning for transparent government – argued that measures already exist to reduce the problems associated with proving damage. The example they gave was the power under section 8(4) of the Official Secrets Act 1920 to exclude members of the public from a hearing if publication of any evidence to be given or of any statement to be made in the course of proceedings would be prejudicial to the national safety. They also stated:

> Removing the requirement to prove damage risks removing any mechanism by which disclosures made in the wider public, and democratic, interest can be defended in court.[154]

4.39 Similarly, the Campaign for Freedom of Information and Article 19 referred to the fact the OSA 1989 allowed evidence to be heard in private, with the public excluded from the court room, if necessary, and asked: "why is this very considerable safeguard insufficient? The consultation is silent on this point".[155]

4.40 Moreover, Alan Rusbridger, former Editor-in-Chief of The Guardian, observed that "the courts are used to dealing with sensitive intelligence information using public interest immunity procedures. I cannot agree with a proposal that the government simply has to assert that the information is sufficiently secret, without any requirement to prove actual or likely damage".[156]

Classified evidence

4.41 We are not able to publish data or details of decisions not to prosecute alleged unauthorised disclosures under the OSA 1989 where that decision related to the requirement to prove damage. This is because public disclosure of information about

---

152 ITN, p 2.

153 BBC, p 2.

154 UK Open Government Network, p 3.

155 Campaign for Freedom of Information and Article 19, p 16.

156 Alan Rusbridger, pp 2 to 3.

the real or potential damage flowing from an alleged unauthorised disclosure could confirm the truth of all or part of that alleged unauthorised disclosure.

4.42 However, we have seen evidence to support the government's concern that the existence of the damage requirement in its current form prevents prosecution of the most harmful disclosures of sensitive information. The following is a hypothetical example that illustrates the risks revealed by the classified evidence.

(1) M, a civil servant not subject to s1(1), leaks a list of alleged employees of the security and intelligence agencies onto a public website. The list is partially accurate, but also erroneously names some HMG staff who do not work for the security and intelligence agencies. This disclosure damages the effectiveness of these agencies, as the identities of several of their employees are now in the public domain. However, it is assessed that confirming the extent of the accuracy of the leaks to illustrate damage would compound the damage done, so M is not prosecuted.

Analysis

4.43 We hope we have clarified the position regarding those who are not Crown servants or government contractors. It was always our intention for damage to remain an essential feature of these offences.

4.44 It is also important to address the concern that we provided insufficient evidence to justify making amendments to the offences. Whilst any legal recommendation requires consideration of future risks, whether or not they have materialised in the past, we recognise the force in the point, and accept that for some consultees a change to the law could only ever be justified by empirical information about the number of prosecutions which have not been commenced due to the damage requirement. Unfortunately, the sensitive nature of this subject matter exacerbates the difficulties which already exist in relation to obtaining empirical evidence of prosecutions which have not been brought. The inability to provide empirical evidence of a problem that has been brought to our attention sometimes arises in the course of the Law Commission's work. For example, when the Law Commission reformed the offence of fraud, there were no statistics we could adduce about the number of prosecutions which had failed due to an inability to prove that the defendant's deception directly caused the victim to part with his or her property. Our analysis in that project relied upon anecdotal evidence provided by stakeholders from across government. However, as we cite at 4.42(1) above, we have had the opportunity to assess evidence on this matter, and that evidence substantiates our concerns.

4.45 In relation to the argument that the damage test acts as an implicit public interest defence, we accept that the question of whether a disclosure was damaging may sometimes coincide with whether it is in the public interest. Damage and the public interest are not necessarily mutually exclusive concepts, however. As we examine in greater detail in Chapter 11, a public interest defence enables a defendant to argue that the public interest in disclosing the information justified any damage that may have resulted. There will therefore be instances where an individual argues that the unauthorised disclosure was in the public interest *despite* the fact it was damaging.

4.46 A significant number of consultees argued that any concerns which might exist about exposing vulnerabilities by having to prove damage or likely damage could be addressed by relying upon section 8(4) of the Official Secrets Act 1920 as applied by section 11(4) of the OSA 1989. This provision enables the judge to exclude the public from the proceedings if publication of any evidence to be given or of any statement to be made in the course of those proceedings would be prejudicial to the national safety. This is not necessarily a complete answer to the problem, however, as noted by the Crown Prosecution Service. For example, even if members of the public are excluded from parts of the proceedings, the material in question must still be heard by the jury. This could give rise to issues about the need for jurors to be vetted and whether jurors might be targeted by hostile agents during or after trial in an effort to gain access to sensitive information.

4.47 The other problem with this approach is that excluding the public from the hearing erodes the principle of open justice. The UK Open Government Network submitted that section 8(4) of the Official Secrets Act 1920 is capable of addressing any concerns. It also submitted that removing the requirement to prove damage risks removing any mechanism by which disclosures made in the wider public, and democratic, interest can be defended in court. Given that the public is most likely to be excluded from those parts of the trial in which evidence of damage is adduced, there will be no public scrutiny of those aspects of the trial which are arguably of the greatest public interest. One of our aims in the Consultation Paper was to find a solution to the problem that was brought to our attention that would have the least impact upon open justice. We doubted whether consultees would welcome an increase in the number of applications to exclude the public from criminal trials. On balance, we took the view that it was preferable to ensure that proceedings could remain as open and transparent as possible. This consideration was one which influenced our provisional proposal based on the conduct model of offence as we described in our Consultation Paper.

Consultation question 6

4.48 Consultation question 6 stated:

> We welcome consultees' views on the suitability of shifting to non-result based offences to replace those offences in the OSA 1989 that require proof or likelihood of damage.[157]

4.49 Dr Ashley Savage agreed with a shift to non-result based offences. Peters and Peters agreed with a shift, but, like the BBC, thought our suggested wording of "capable of damaging" was too broad.[158] The Bar Council and Criminal Bar Association queried whether a shift to non-result based offences would achieve its objectives, as did the Government Response.

4.50 There was a negative response to this consultation question from News Group Newspapers, Guardian News and Media, Liberty, Associated Newspapers, UK Open

---

157 Consultation Paper, para 3.164.

158 Peters and Peter, p 7.

Government Network, ITN, Campaign for Freedom of Information/Article 19 and Campaign Against Censorship.

4.51 The Crown Prosecution Service suggested that the UK's intelligence community was better placed than the CPS to comment on this question.[159]

4.52 In their joint response, the Bar Council and the Criminal Bar Association stated:

> The proposals at 3.161 do not meet the perceived problem of proving damage in practice. In order to prove that the defendant knew or had reasonable grounds to believe that disclosure is capable of causing damage, the prosecutor will in the ordinary course have to prove the potential for damage. It is from that evidence that the inference of knowledge is often drawn. The practical difference between proving reasonable grounds to believe that disclosure could cause damage and proving that disclosure could cause damage may be less than envisaged. Both involve an objective assessment of potential damage.[160]

4.53 Peters and Peters stated:

> …in relation to the Commission's proposed redrafts of the offences (at page 83 of the Consultation Paper), we question the use of the phrase "capable of damaging" in reference to the probability (as understood by the defendant at the time) that the relevant damage would result from the defendant's disclosure. Should it suffice if the defendant knew that there was a remote possibility that his disclosure might damage security and intelligence, defence or international relations? We suggest that a higher probability of harmful consequences, and the defendant's awareness of these potential consequences, should be required here.[161]

4.54 In disagreeing with the proposal to shift to a non-result based offence, News Group Newspapers made the following point:

> NGN considers that the structure currently contained in section 5(3) of the OSA 1989 should be maintained. In addition, NGN draws attention to the fact that the proposed redrafting set out in paragraph 3.161 imposes a lower threshold of knowledge / belief than is currently contained in section 5(3)(b) of the 1989 Act. Paragraph 3.161 proposes that 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 or having reasonable grounds to believe that that disclosure *"is capable of"* damaging security and intelligence, defence or international relations. By contrast, section 5(3)(b) requires the Defendant to have made the disclosure knowing, or having reasonable cause to believe, that it *"would"* be damaging.[162]

---

159 Crown Prosecution Service, para 14.

160 Bar Council and Criminal Bar Association, para 42.

161 Peters and Peters, p 7.

162 News Group Newspapers, para 12.

4.55 Guardian News and Media described a shift to non-result based offences as a "significant weakening" of the current legal test:

> It means that a disclosure which is *unlikely* to cause damage may nevertheless be an offence because in circumstances that are highly unlikely to ever arise, it *might* cause damage. This may mean that if a journalist has been told by an official that a disclosure would be damaging, but has good reason not to believe it, they might still commit an offence – because having been told, they may now have reasonable cause to believe that it is 'capable' of being so.[163]

4.56 In strongly disagreeing with this consultation question, a member of the public, Damien Shannon, argued that it may be "adduced only to allow the executive to escape the responsibility to demonstrate that there has been any deleterious consequence to a given disclosure".[164]

4.57 Associated Newspapers gave a series of examples where removing proof of damage would make it easier than it currently is to charge people who make disclosures that were arguably in the public interest:

> ANL's concerns are not assuaged by the Law Commission's recommendations [sic] on the introduction of a requirement to prove subjective fault… While subjective fault is usually part of the justification for criminalising conduct, it is not a comparable alternative justification for criminalising the conduct in issue – ie an alternative to actual or likely harm to an important public interest. The societal harm involved in criminalising journalists and their sources may in principle be justified by harm to such a public interest. It cannot be justified by pointing simply at subjective fault on the part of the individual charged.
>
> In any event it is unclear how this is supposed to remedy the perceived problem… If proving that the information is of a <u>type</u> *likely* to have the relevant damaging effect is problematic so must proving this sort of subjective fault.
>
> The removal of this objective requirement from the ss.5 and 6 defences is particularly worrying...[165]

4.58 The BBC observed that:

> A reformation of the offences should also serve to safeguard media defendants in circumstances where the primary intention behind disclosure is to highlight a matter of significant public interest rather than to cause damage to matters of national security. Thus, we are strongly of the view that the proposal to add a *mens rea* element to the offence must be accompanied by a public interest defence in the event that the harm test is removed.[166]

---

163 Guardian News and Media, pp 4 to 5 [emphasis in original].

164 Damien Shannon, p 2.

165 Associated Newspapers, paras 37 to 39 [emphasis in original].

166 BBC, p 2 [emphasis in original].

4.59 ITN argued that removing the requirement to prove damage would interfere with the editorial process:

> At present the editorial decision-making process takes into account the likelihood of damage alongside public interest. However, moving from evidence of actual damage in terms of the offence to an awareness or knowledge that the information may be detrimental to national security reduces the burden of proof. It may reduce the burden on the state but in so doing opens the door for unsubstantiated claims of damage. This fundamentally disrupts the editorial decision-making process introducing far more risk and leading to a likely chilling effect on the publication of stories that are automatically more likely to incur significant penalties – specifically penalties levied at individual journalists rather than media organisations.[167]

4.60 Liberty expressed strong opposition, submitting:

> We urge the Law Commission to abandon its proposals to remove the damages threshold, and recommend instead that any offence of unauthorised disclosure must only attach to information the disclosure of which would cause identifiable, serious harm to national security.[168]

4.61 Professor David Leigh, Anthony Sampson Professor in Reporting at City, University of London disagreed with idea of "dropping the damage requirement… because the effect will be to criminalise responsible journalists".[169]

4.62 The Campaign Against Censorship responded:

> Our view is that proof of damage is an essential component of an offence under Official Secrets legislation. People should not be prosecuted for damage that they only might have done.[170]

4.63 The Government Response expressed a lack of confidence as to whether the practical effect of our proposals would be significant:

> We question whether the ability to prosecute damaging unauthorised disclosures would be materially enhanced by moving from a requirement that the disclosure was *likely* to cause damage (i.e. there was a real likelihood that it would have this effect to a requirement that the defendant *knew that the disclosure was capable* of causing damage. We see that a requirement to prove knowledge of "capability" to damage may in principle place a lower burden on the prosecution than a requirement to prove "likelihood" to damage. But we believe that in practice, in order to secure a conviction, the Crown would need in either case to adduce evidence to demonstrate the potentially damaging effect of the disclosure. This is because a person can only *know* that their disclosure is capable of causing damage if it is in fact so capable, and the Crown will need to prove that capability in order to prove that the defendant knew or must have known of it. In some cases, it might be possible to prove the

---

167 ITN, pp 5 to 6.

168 Liberty, p 15.

169 Professor David Leigh, by email.

170 Campaign Against Censorship, by email.

potential of a disclosure to cause damage by means of general evidence that is not in itself sensitive. But this is unlikely to be the usual position. Rather, we would expect the courts to require a defendant's knowledge of the capability of their disclosure to cause damage to be strictly proved by specific evidence.[171]

Provisional conclusion 10

4.64 Provisional conclusion 10 stated:

> 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?[172]

4.65 The Bar Council and Criminal Bar Association, Dr Ashley Savage, Peters and Peters and Trinity Mirror all agreed with provisional conclusion 10. The Crown Prosecution Service gave their qualified support, observing that there would be "many arguments about what constitutes knowledge or reasonable grounds to believe that the disclosure is capable of causing damage".[173]

4.66 Peters and Peters stated:

> These are serious criminal offences in relation to which the Commission proposes to increase the applicable maximum sentence. Furthermore, there is currently no public interest defence and the Commission does not recommend introducing one. It is critical, therefore, that the provisions should only apply where there is a sufficient level of culpability on the part of the person making the disclosure.[174]

4.67 The BBC supported the proposal to add a subjective fault element to the offences in the OSA 1989, but expressed a preference for the phrase "likely to materially damage", noting that:

> … we believe that the suggested drafting … is too wide, in particular the wording "knowing that / having reasonable grounds to believe that disclosure is ***capable of*** damaging security and intelligence, defence or international relations". The use of the words "capable of" would significantly lower the threshold of criminal liability as it could encompass disclosure which has only a remote possibility of causing damage. [emphasis added][175]

4.68 News Group Newspapers and the News Media Association argued that objective damage *and* subjective mens rea ought to be a feature of the offence.

4.69 News Group Newspapers stated:

---

171 Government Response, pp 9 to 10 [emphasis in original].

172 Consultation Paper, para 3.151.

173 Crown Prosecution Service, p 4.

174 Peters and Peters, p 6.

175 BBC, p 2.

NGN agrees with this conclusion. Similar to the position regarding section 1 of the Official Secrets Act 1911, as set out above, NGN is in favour of a requirement that the Defendant only commits an offence where he knows or has reasonable grounds to believe that disclosure would cause damage, and intends thereby to cause damage or is reckless as to whether such damage would be caused. However, NGN is not in favour of the simultaneous removal of the requirement that the disclosure actually be damaging.[176]

4.70 The News Media Association stated that they:

> … would not object to the addition of a mental element, such that the Act would require the prosecution to prove both the new element of damaging intent and that damage was caused by the disclosure made with such intent. However, the substitution of the former for the latter is unacceptable.[177]

4.71 The Government Response stated:

> We strongly agree with this provisional conclusion for the reasons given by the Commission. But this is on the assumption that the fault element will remain as construed in *Keogh.* If the fault element were raised, this would compound the difficulties of prosecuting the offence.
>
> We are not persuaded that having reasonable grounds to believe is a subjective fault element. If someone is liable to conviction because they had reasonable grounds to believe, although they did not *in fact* believe, that would seem to be an objective rather than a subjective basis of liability.[178]

Analysis

4.72 A number of consultees were only in favour of the provisional conclusion provided it was coupled with the requirement to prove damage or a likelihood of damage. This provisional conclusion was not intended to be viewed in isolation, however. We asked consultees for their views on whether a fault element should be included because, in the event that consultees agreed with our provisional conclusion that the offences be remodelled to focus on conduct rather than result, we were keen to ensure that there was no dilution of the threshold of culpability that must be crossed before an offence is committed. Assuming the offences retained the damage requirement, there would be no need to insert a fault element.

4.73 As we have explained, our provisional conclusions were cumulative: a shift to a non-result based offence, combined with an increased fault requirement. Our view was that this would strike the right balance between ensuring that a prosecution could be brought in appropriate cases whilst not diluting the threshold of culpability. Very few consultees agreed with the proposals viewed as a whole. For example, News Group Newspapers welcomed an increased fault requirement, but not if it was combined with a shift to a non-result based model of offence.

---

176 News Group Newspapers, para 10.

177 News Media Association, p 11.

178 Government Response, p 9.

4.74 In evaluating this provisional conclusion, we believe that some consultees have conflated damage with a defence of public interest. A public interest defence permits a defendant to argue that *despite* any damage caused, the public interest in disclosure outweighed the public interest in keeping the information confidential. One way to rebut this is for the prosecution to adduce evidence of the extent of the damage. This, however, may give rise to the problems which were brought to our attention during our pre-consultation phase.

4.75 A number of consultees took issue with the use of the words "capable of" in the examples we gave at paragraph 3.161 of our Consultation Paper. We repeat them here:

(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.

4.76 These examples were expressed to be only indicative of how the offences could be reformulated so as to focus on the defendant's state of mind when he or she disclosed the information in question without lawful authority. There are other ways the offences could be reformulated, for example by requiring the defendant to have intended or been reckless as to whether disclosing the information would be capable of damaging a protected interest.

4.77 We do acknowledge the difficulty inherent in this task: a balance will need to be struck between a test that retains an adequate threshold of liability without in practice creating the same problems of proof from which the damage requirement presently suffers. To the latter point, it is nonetheless worth noting that section 3(3)(a) of the 1989 Act already contains a provision that the mere fact that a document is confidential may be sufficient to establish damage (for the purposes of the section 3(1)(b) offence alone). The same reasoning could well apply to the defendant's awareness of the risk of damage. Nonetheless, we recognised in the Consultation Paper that more detailed work would need to be undertaken when it came to drafting a Bill, and that a consensus would need to be reached as to which fault element (such as intention, recklessness or reasonable grounds to believe) is the most appropriate to rely upon in this context.

4.78 There would also be advantages in incorporating fault as an explicit element of the offence (as is the case in sections 5 and 6) rather than relying on absence of fault as a defence. First, it aligns the various offences. Secondly, and more importantly, it means that the offences no longer contain a reverse burden of proof as to the mental element that needs to be 'read down'.

4.79 In short, there are some individuals who owe a special duty to safeguard information deriving from their position. One such individual might make an unauthorised

disclosure, realising there is a risk of harm to a protected interest. We continue to believe that it is undesirable, as a matter of principle, for such an individual to avoid prosecution on the basis that proving his or her guilt requires the prosecution to compound the damage caused by the initial unauthorised disclosure. This is heavily influenced by the fact that those offences in the OSA 1989 which we are currently discussing can only be committed by Crown servants, government contractors and notified persons. We therefore continue to believe there is merit in the model of offence we described in our Consultation Paper. We adopted the same approach in the Report which precipitated the enactment of the Fraud Act 2006, so there is precedent for adopting this model.

4.80 However, we do recognise the weight of consultees' strong opposition to this recommendation (albeit that some of that opposition was directed towards changes to sections 5 and 6, which we are not recommending). It is our view that the majority of these concerns will have been addressed by fortifying and balancing this recommendation with the public interest disclosure recommendations that we make later in the Report.

Recommendation 11.

4.81 Those offences under the Official Secrets Act 1989 that relate to Crown servants or government contractors and that require proof or likelihood of damage (section 1(3); section 2(1); section 3(1); section 4(1)) should no longer require such proof or likelihood.

4.82 Instead, there should be an explicit subjective fault element. Further work will be required to determine the most appropriate fault element (ie that the defendant (i) knew; (ii) believed; or (iii) was reckless as to whether the disclosure (a) would cause damage; (b) was likely to cause damage; (c) risked causing damage; or (d) was capable of causing damage).

4.83 Sections 5 and 6 should continue to be based on proof or likelihood of damage.

Chapter 5: Other Reforms to the Official Secrets Act 1989

INTRODUCTION

5.1 Having set out the current law, and examined the damage requirement in Chapter 4, in this Chapter we consider the other provisional proposals for reform of the Official Secrets Act 1989 that we made in our Consultation Paper. We examine and analyse consultees' responses before making a series of recommendations.

5.2 We deal with the following issues:

(1) liability under section 1(1) of the Official Secrets Act 1989;

(2) reform of the notification process and the definition of "member of the security and intelligence agencies";

(3) the maximum sentence available under the Official Secrets Act 1989;

(4) access to legal advice;

(5) the need for a prior publication offence;

(6) the need to amend the categories of information currently protected;

(7) extending the protection of the Act to sensitive economic information;

(8) extraterritoriality; and

(9) the optimal legislative vehicle for reform.

LIABILITY FOR THE SECURITY AND INTELLIGENCE AGENCIES

5.3 The offence contrary to section 1(1) of the Official Secrets Act 1989 ("OSA 1989") has no damage requirement. Section 1(1) provides:

> 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.

5.4 This offence is, however, subject to a defence in section 1(5) of the OSA 1989 of not knowing and having no reasonable cause to believe that the information, document or

article in question related to security or intelligence. In the case of *R v Keogh*,[179] which we discussed in our Consultation Paper, the Court of Appeal noted that "reasonable cause to believe" would be decided upon an assessment of wholly objective fact.[180]

5.5 A similar expression, "reasonable grounds to suspect", was considered in *R v Saik*[181] with regard to the offence of conspiracy to launder money under section 1(1) of the Criminal Law Act 1977. The Court held that "reasonable grounds to suspect" required a subjective suspicion supported by objective grounds.[182] Subsequently, however, in a more closely related context (considering "reasonable cause to suspect" in section 17 of the Terrorism Act 2000), the Supreme Court in *R v Sally Lane and John Letts*[183] noted that:

> it is not possible to read … *R v Saik* ... as laying down a universal proposition that if a statute speaks of a person having "reasonable cause to suspect", that will always assume that he has to have an actual suspicion.[184]

5.6 The Court held that while actual suspicion is not required, it is to be interpreted as imposing a cumulative test, combining subjective awareness – of the information available to the accused – based on objectively verifiable grounds.[185] Given this case law since *Keogh*, it is likely that the approach to interpreting the defence under section 1(5) of the OSA 1989 would be based on this cumulative test. The jury would be required to undertake a (i) a subjective assessment of the information available to the accused that might give reasonable cause to believe (or indeed, the lack thereof) and (ii) a determination – on objective grounds – as to whether there was or was not reasonable cause to believe that the information related to security or intelligence.

5.7 In our Consultation Paper, we provisionally concluded that there was force in the argument that membership of the security and intelligence agencies carries a special and inescapable duty to protect official government data. When an individual chooses to accept employment as a member of the security and intelligences, he or she is aware that it is subject to the limitations imposed by section 1(1). We did not propose any amendment of the defence currently contained in section 1(5) of the OSA 1989.[186]

Provisional conclusion 11

5.8 Provisional conclusion 11 asked:

---

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

180 See Consultation Paper, paras 3.74 to 3.90. Although this particular case related to sections 2(3) and 2(4) of the OSA 1989, as we discussed in our Consultation Paper, it is likely the same reasoning would apply in relation to other sections of the Act with similar phrasing.

181 [2006] UKHL 18; [2007] 1 AC 18.

182 *R v Saik* [2006] UKHL 18; [2007] 1 AC 18 at [52] to [53].

183 [2018] UKSC 36.

184 *R v Sally Lane and John Letts* [2018] UKSC 36 at [17].

185 *R v Sally Lane and John Letts* [2018] UKSC 36 at [24].

186 Consultation Paper, paras 3.165 to 3.166.

> With respect to members of the security and intelligence agencies and notified persons, the offences should continue to be subject to strict liability. Do consultees agree?[187]

Consultation responses

5.9 The Crown Prosecution Service and Bar Council and Criminal Bar Association agreed with this provisional conclusion, as did the Government Response and the Campaign Against Censorship.[188] Dr Ashley Savage agreed that the role of individuals working within the security and intelligence services should be reflected in the legislation, but added:

> If the Law Commission were to conclude that the strict liability offences should be maintained, to ensure compliance with the European Convention, it is suggested that the special restriction imposed on members of the security and intelligence services must be supported by an authorised disclosure mechanism underpinned by statute to allow individuals to raise concerns.[189]

5.10 Peters and Peters disagreed with provisional conclusion 11, arguing that serious offences should not in principle be ones of strict liability, especially where there was no public interest defence.[190] Oliver Butler did not agree that members of the security and intelligence services should continue to be subject to strict liability:

> a negligence standard is sufficiently flexible to take into account the responsibility of the official in question. Where a member of the security and intelligence service makes an unauthorised disclosure where, even by the high standards to which they must be held, he or she was not negligent to make that disclosure, then I do not think he or she should be held liable.[191]

5.11 The News Media Association argued that an intention to make damaging disclosures should be required, along with proof of damage, for members of the security and intelligence services.[192] The Institute of Employment Rights argued that strict liability was undesirable as it "denies a defence of public interest to those in the services who may have information relating to the conduct of the services which may relate to illegality or inefficiency …".[193]

5.12 Liberty argued that:

---

187 Consultation Paper, para 3.167.

188 Campaign Against Censorship was established as the Free Art Legal Fund in 1967. They are an organisation opposing censorship and promoting freedom of expression in the UK.

189 Dr Ashley Savage, para 12.

190 Peters and Peters, p 7.

191 Oliver Butler, p 7.

192 News Media Association, p 17.

193 The Institute of Employment Rights, p 20. This appears to conflate the fault element with the public interest defence. It would be possible to intend a disclosure to be damaging and also in the public interest, for instance, if damage were considered to be a necessary evil to expose illegality.

> The arbitrary, blanket prohibition on disclosure of any information a person acquires as a result of their work in the security and intelligence services results in … absurd consequences … Not only are revelations in the public interest punished, but … disclosure of a document by a member of the Security Services may be an offence, whilst disclosure of *the same document* by a former civil servant in the Home Office may not be.[194]

5.13 Peters and Peters also argued that because the notification procedure was "nebulous" and "open to being interpreted broadly", strict liability should not necessarily apply to all notified persons.[195] We return to the notification process below.

Analysis

5.14 We remain of the view that members of the security and intelligence agencies, and those notified that they are subject to the provisions of section 1, should be subject to a stricter legal regime than other Crown servants. The work undertaken by the security and intelligence agencies sets them apart from those in other government departments. This is reflected by section 1(1) of the OSA 1989. It is important to bear in mind that this provision does not impose absolute liability, given the existence of the defence in section 1(5). This defence acts as a safeguard against conduct that could be characterised as being merely negligent. It is also important to note that strict liability for members of the security and intelligence agencies only applies where the unauthorised disclosure relates to security or intelligence. If the member makes an unauthorised disclosure relating to another category protected by the OSA 1989 (ie a different OSA 1989 offence), they will be liable on the same basis as other Crown servants and government contractors. In relation to the point made by Dr Ashley Savage, we agree with him and discuss authorised disclosure routes more fully in Chapter 10.

5.15 Although we have recommended no change to the offence in section 1(1) of the OSA 1989, we do believe that the recommendations we make in relation to the question of the role of the statutory commissioner and whether there ought to be a public interest defence (which would apply to the section 1(1) offence) will address some of the concerns raised by consultees about the impact of not requiring proof of damage in respect of members of the security and intelligence agencies (see Part III).

5.16 We note the comments raised by Peters and Peters about the extent to which notified persons are subject to strict liability. We address the notification procedure below and make recommendations to reform and clarify the provisions concerning notified persons. Given the reasons why a person would be subject to notification, we take the view that there should be no change to section 1 as it applies to notified persons. Furthermore, we consider that notified persons should be required to report concerns to the statutory commissioner that we recommend be introduced (see Chapter 10) on the same basis that we recommend for members of the security and intelligence agencies. We discuss our proposals relating to the role of the statutory commissioner in Chapter 10.

---

194 Liberty, para 53.

195 Peters and Peters, p 7.

Recommendation 12.

5.17 The offence contrary to section 1(1) of the Official Secrets Act 1989 should not be amended to require proof that the disclosure was damaging.

5.18 The "defence", currently contained in section 1(5) of the Official Secrets Act 1989, of not knowing and having no reasonable grounds to believe that the material disclosed related to security or intelligence, should continue to apply.

REFORM OF THE NOTIFICATION PROCESS AND THE DEFINITION OF "MEMBER OF THE SECURITY AND INTELLIGENCE AGENCIES"

5.19 Section 1(6) of the OSA 1989 provides that individuals can be made subject to section 1(1) of the OSA 1989 by written notification 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 the subsection". For example, members of the Intelligence and Security Committee of Parliament are notified persons.

5.20 The Home Office is responsible for processing notifications for the security and intelligence agencies, the police and the Home Office itself. Other departments issue their own notifications as required. The notification must be served in writing. Notification remains in force for five years from the date on which it is served and is subject to renewal.[196]

5.21 In our Consultation Paper, we noted that concerns had been expressed to us during pre-consultation that the notification procedure was overly bureaucratic, and that this could result in failures to notify effectively and appropriately. Stakeholders representing various Government departments also expressed concern that the delay in the procedure may present problems by failing to keep pace with internal restructuring within departments. We also noted the concerns that had been expressed to us that the power to extend the scope of "Crown servant" in sections 12(1)(f) and (g) of the OSA 1989 was "bureaucratic and cumbersome and in need of improvement".[197] Finally, we referred to the fact that the term "member of the security and intelligence agencies is not defined", which meant that its intended meaning was obscure (for example, it is not clear that it applies widely enough in relation to those who, while not employees of the intelligence services, are nonetheless involved in intelligence and security work by virtue of, say, a secondment or as a Minister of a relevant Department).

Provisional conclusion 12

5.22 Provisional conclusion 12 stated:

---

196 Official Secrets Act 1989, s 1(7).

197 CP, paras 3.168 to 3.177.

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

5.23 Consultation question 7 asked:

> 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?
>
> (a) 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).
>
> (b) 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.
>
> (c) 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.

5.24 Since publishing our Consultation Paper, we have been able to obtain statistics on the number of notified persons. As of February 2018, there were 2,813 people notified pursuant to section 1(6) of the OSA 1989. The following data was provided by the Home Office, one of the Departments with responsibility for administering the notification process:

Year	New notifications issued	Notifications renewed	Notifications revoked
2013	960	5	114
2014	642	0	227
2015	535	6	275

Year	New notifications issued	Notifications renewed	Notifications revoked
2016	562	0	377

Consultation responses

5.25 Of the relatively few consultees who responded to this series of questions, most agreed with provisional conclusion 12. The News Media Association stated:

> The criminal law requires certainty and it is important that it is clear to whom the Act applies to any potential subject and to any third party.[198]

5.26 The Bar Council and Criminal Bar Association joint response suggested that a person should be asked to countersign a notification so there is no doubt they are subject to section 1(1):

> The overriding principle should be clarity in the process both as a protection to the affected persons and to the sensitive information.[199]

5.27 Peters and Peters accepted the need to improve the flexibility of the notification procedure but also stressed that it was important that individuals were made explicitly aware of their obligations.[200]

5.28 The Crown Prosecution Service agreed with the need for reform to improve efficiency, and were in favour of new guidance to clarify when a person should be subject to notification and an extension of the notification period. They considered that replacing notification with an expanded section 1(1) to cover anyone who has, or has had, access to security and intelligence information by virtue of their office or employment or contract of services "may be a step too far".[201]

5.29 Whistleblowers UK was of the view that the "notified persons list should be tightly drawn so as to reflect only national security and should be subject to frequent review", and that there was a need for safeguards to prevent abuse of process.[202]

5.30 Campaign Against Censorship expressed concern that reform of the notification process had the potential to make individuals retrospectively liable for their handling of information at some time in the past.[203] We do not consider that the notification process has ever been or even could be used in this way.

---

198 News Media Association, p 17.

199 The Bar Council and Criminal Bar Association, p 9 to 10.

200 Peters and Peters, p 8.

201 Crown Prosecution Service, p 5.

202 Whistleblowers UK, p 2

203 Campaign Against Censorship, by email.

5.31 Public Concern at Work stated:

> Whilst we agree that the notification process is in need of reform, we submit that there are substantial failings which necessitate this rather than just a need for efficiency. ... Currently, the notification process can be used as a means of potentially intimidating whistleblowers. …[204]
>
> The basic principle of fully informing civil servants of the duties and responsibilities under the OSA is certainly a practice that should be encouraged – this is an area where a blanket approach to the signing of the OSA does not provide a solution and does not sit with the proper accountability of government departments. Guidance and training should also be considered for those departments that deal with protected information on a regular basis, so that there is a consistent approach across Government.[205]

5.32 The Trinity Mirror contended:

> the scope of those required to sign the Official Secrets Act should not be extended to surround government with a cloak of secrecy. The categories of person who need to be restricted by the act must not exceed what is strictly necessary to protect national security.[206]

5.33 Dr Ashley Savage's response was detailed and is worth setting out in full.[207] In relation to whether the term "member of the security and intelligence services" ought to be amended, he stated:

> This would be a sensible approach. It would also be appropriate to consider whether to use the term 'worker' or 'a person who works for' the security and intelligence services should be used as an alternative to avoid any suggested interpretation of the term "employee" to mean a person who has served a qualifying period of employment. It is further suggested that any term used should be supported with a statutory definition and this should be consistent with interpretations found in Employment Law.[208]

5.34 In relation to the notification process, he submitted:

> The author is unable to provide a full view on the notification of individuals. However, it is submitted that the Law Commission's provisional conclusion that notified persons should remain is correct. Notification serves a useful purpose particularly where individuals have been notified but are not made subject to Developed Vetting. For example, by notifying members of the Intelligence and Security Committee but

---

204 Public Concern at Work, para 10.

205 Public Concern at Work, para 14.

206 The Trinity Mirror, by email.

207 Dr Ashley Savage, paras 15 to 16. Dr Savage is a research fellow at the International Anti-Corruption Academy, Austria and former lecturer at the University of Liverpool with particular expertise in this area.

208 Dr Ashley Savage, para 14.

not making them subject to Developed Vetting the system arguably allows members to retain independence from the establishment.

If notification is proposed to continue, it would be sensible to review the justification behind notified persons being subject to the same requirements of strict liability as members of the security and intelligence agencies. Whilst there are clear policy justifications to suggest that security and intelligence information should be protected at the highest level, there is also the potential policy argument to suggest that notified office holders tasked with maintaining oversight of the agencies should be able to publish information concerning wrongdoing in the public domain in order to fulfil their democratic mandate. If authorisation to publish is refused by the government of the day, notification resulting in the committal of a strict liability offence appears to be overly restrictive. The author appreciates that the circumstances where this might occur may be limited.[209]

5.35 The Government Response stated:

> We believe the law should be clarified to make explicit that a "member" of the security and intelligence agencies includes any individual employed or contracted by the agencies or seconded or attached to them.
>
> Guidance has been in place since the commencement of the notification regime. The problem lies not in the guidance itself but in the difficulty of applying it given the many and varied scenarios in which individuals may have legitimate access to security and intelligence material. For this reason, we do not believe that revised guidance provides anything more than a partial answer to the problems with the notification regime. Extending the notification period would also be of limited assistance in reducing the bureaucratic burden of the regime, given the requirement to cancel a notification when it is no longer needed. We therefore strongly prefer the Commission's second option, or defining the class of people who are caught by the section 1(1) offence. We suggest that for simplicity the class should cover any Crown servant or government contractor who has access to security or intelligence material in the course of their office or employment or under a contract for services. But to cover all eventualities we also favour retaining the power to notify individuals not within the defined class where their access to security and intelligence material makes that appropriate.

5.36 No consultee provided a response to the provisional conclusion that the process for expanding the definition of Crown servant ought to be streamlined and should be possible to make an officeholder a Crown servant for the purposes of the OSA 1989 by way of primary legislation, in addition to the process set out in section 12 of the Act.

Analysis

5.37 We take the view that it is valuable to maintain "notified persons" as a category within section 1(1) of the OSA 1989. We also accept the point that was made by a number of consultees that it is crucial for notified persons to be aware of the fact they have been made subject to the stricter regime in section 1(1) of the OSA 1989. Given that notification must be provided in writing to the individual in question, we do not have

---

209 Dr Ashley Savage, paras 15 and 16.

the impression that there are problems in this regard. Furthermore, in relation to the point raised by the Bar Council and Criminal Bar Association, our understanding is that individuals are already asked to sign to confirm they have been notified. We believe there is merit in publishing the guidance that informs when a person ought to be notified. This would bring a degree of transparency to what is currently a poorly-understood process.

5.38 The consequences of notification are potentially serious. Given that this is the case, the ability to notify should be kept within narrow parameters. We therefore agree with the view expressed by the Crown Prosecution Service that replacing notification with an expanded version of section 1(1) of the OSA 1989 would be disproportionate, as it would potentially bring a multitude of individuals within the scope of that offence. It would also be difficult to keep track of those individuals who are subject to section 1(1). This would be undesirable as a matter of legal certainty, as it risks individuals not being aware that they are subject to section 1(1) of the OSA 1989.

5.39 In terms of the definition of "member", the definition proposed in the Government Response appears to be sufficiently clear and precise (above at 5.35). As Dr Ashley Savage pointed out, however, the employment law implications of using the term "employee" would need to be carefully considered should it be adopted in future.[210]

5.40 Consultation Question 7(c) above (definition of a Crown servant) arose from a concern that there was no way in primary legislation to specify that certain categories of person are Crown servants for the purposes of the OSA 1989, leaving only the "bureaucratic and cumbersome"[211] process in sections 12(1)(f) and 12(1)(g) of that Act. On reflection, this concern was without basis. It is clearly possible for Parliament, as the supreme legislative body of the United Kingdom, to pass legislation to this effect (see, for example, Schedule 7 to the Energy Act 2013[212]). We therefore make no further recommendation on this point.

Recommendation 13.

5.41 The definition of "member" of the security and intelligence services should be clarified to mean any individual employed or contracted by the security and intelligence services or seconded or attached to them.

5.42 There should be a statutory requirement to publish guidance on the notification process. The guidance should state which categories of office are subject to notification and how an individual can challenge a decision to notify him or her.

---

210 The term "employee" may be too restrictive if taken to mean "someone who has passed a qualifying period of employment" and would need to be consistent with employment law. Dr Ashley Savage proposes using some other term (for example, "worker") to avoid this pitfall.

211 CP, para 3.176.

212 Sch 7, para 5 of the Energy Act 2013 says "service as a member of the ONR [Office for Nuclear Regulation] is not service in the civil service of the state, but this is subject to paragraph 6". Para 6 then says "Members of the ONR are to be regarded as Crown servants for the purposes of the Official Secrets Act 1989".

SENTENCING

5.43 The maximum sentence currently available for most of the offences contained in the OSA 1989 is two years' imprisonment. Section 10 states:

> (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.

5.44 A person guilty of an offence under section 8(1), (4) or (5) above is liable on summary conviction to imprisonment for a term not exceeding three months or a fine not exceeding level 5 on the standard scale (now unlimited) or both.

5.45 Our Consultation Paper suggested that the maximum sentence available in the OSA 1989 might not adequately reflect the culpability of an individual in the most egregious cases. A single unauthorised disclosure of information relating to security or intelligence could result in serious harm or perhaps even death. For example, a police officer could disclose information relating to the whereabouts of a protected witness, which not only jeopardises the life of the witness, but could also fatally undermine the investigation and prosecution of a serious criminal offence. We considered a two-year sentence to be inadequate in the most serious cases. However, we made no provisional proposal as to what the sentence should be and we make no associated recommendation in this Report.

5.46 We also observed how advances in technology mean that it is now possible to disclose vast amounts of information contrary to the OSA 1989, leading to the potential for greater harm.[213] The case of Daniel Houghton provides a good example of why the two-year maximum sentence may be inadequate. As we discussed in our Consultation Paper, Mr Houghton offered to sell staff lists from the Secret Intelligence Service. Doing so could potentially have placed lives in jeopardy.

5.47 We observed that the maximum sentence appeared to be low when compared to the maximum available sentence in similar jurisdictions. For example, in Canada, the maximum sentence for an offence contrary to section 4 of the Security and Information Act 2001 is 14 years' imprisonment. A number of consultees appeared to believe we were concluding that the maximum sentence should therefore be 14 years. We did not provisionally conclude that the maximum sentence in domestic law ought to be 14 years' imprisonment, nor did we ask consultees for their views on whether it ought to be raised to 14 years.

Provisional conclusion 13

5.48 Provisional conclusion 13 stated:

---

213 CP, paras 3.180 to 3.189.

We provisionally conclude that the maximum sentences currently available for the main 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?

Consultation responses

5.49 The Crown Prosecution Service agreed with this provisional conclusion,[214] as did the Government Response, which stated:

> The unauthorised disclosure of security and intelligence information can lead to risk of life (of agents or intelligence officers, or of people wrongly identified as such), compromise vital national security intelligence gathering techniques, alert terrorist and serious crime intelligence targets to the interests of the authorities, and cause serious and long term damage to critical international intelligence relationships. We believe that if the maximum sentences for the offences of unauthorised disclosure were raised to 14 years' imprisonment, in line with the sentences available for the spying offence under section 1 of the OSA 1911, this would enable a sentencing court to deal appropriately with serious cases of this sort. We also believe it would be desirable for there to be a review of the circumstances in which a Crown servant may by law forfeit some or all of their pension on conviction under the 1989 Act, in order to ensure that forfeiture is available in an appropriate case.

5.50 Peters and Peters agreed that the availability of a higher maximum sentence would be appropriate:

> The harm caused by an unauthorised disclosure may range from negligible to catastrophic and the culpability of the person making the disclosure from low (in the case of an individual who considers there to be a minimal risk to the national security) to high (where a disclosure is made for the purpose of causing harm to UK interests). We agree with the Commission that a higher maximum sentence, perhaps of five years' imprisonment, would allow for greater differentiation in sentencing between the most and least serious cases and would bring the penalty for these offences in line with the maximum sentence for unauthorised disclosure under sections 57 to 59 of the Investigatory Powers Act 2016. This is the approach that we suggest the Commission should take.[215]

5.51 The BBC considered that the current maximum sentence was sufficient in the vast majority of cases, but they appreciated that it might not be for very exceptionally serious cases. They also stated:

> If the Commission does conclude that the maximum sentence should be increased for such exceptional cases, we would like to make it clear that we do not think that this should be used as a rationale for re-setting sentences more widely.[216]

---

214 Crown Prosecution Service, p 6.

215 Peters and Peters, p 9.

216 BBC, p 3.

5.52 Dr Ashley Savage welcomed a review of maximum sentences, but cautioned against an increase, particularly if it was not accompanied by a "robust and viable authorised whistleblowing mechanisms and a narrowly defined public interest defence".[217]

5.53 The Bar Council and Criminal Bar Association did not wish to express a view on sentencing policy but stated there should be a "clear rationale" before any increase in the maximum sentence was proposed.[218]

5.54 Other consultees, such as Whistleblowers UK, the UK Open Government Network and The Trinity Mirror, were opposed to an increase in maximum sentences.[219] Liberty argued that an increase in maximum sentences was unnecessary as more serious cases could be dealt with under the OSA 1911, which carries a 14-year maximum sentence. Furthermore:

> [The Law Commission's] mention of Canada's 14-year sentences is apt to mislead, since Canadian law provides for a public interest defence.[220]

5.55 Guardian News and Media made a similar point to Liberty and questioned the validity of the Canadian example. Additionally, they pointed out that many countries limit the maximum sentence to five years' imprisonment in the absence of espionage, treason, delivery to a foreign state, or an intention to prejudice security or defence. Guardian News and Media stated that a higher sentence "would place the UK media at a considerable international competitive disadvantage".[221]

5.56 The Courage Foundation argued that sentencing had to be considered in the context of an employee facing other penalties, such as loss of employment. They did not consider the case had been made for increased criminal penalties. Further, they stated:

> The history of prosecutions under the 1989 Act does not, to the best of our knowledge, reveal an example of someone being sentenced to the maximum 2 years, still less an instance where the maximum sentence has been stated to be inadequate.[222]

5.57 Media consultees tended to focus on the effect an increase in sentences could have on freedom of expression. The News Media Association considered that current sentences were already a major deterrent on whistleblowing.[223]

5.58 Associated Newspapers stated:

---

217 Dr Ashley Savage, para 18.

218 The Bar Council and Criminal Bar Association, p 10.

219 Whistleblowers UK, p 2; UK Open Government Network, p 3; The Trinity Mirror, by email.

220 Liberty, para 55.

221 Guardian News and Media, pp 65 to 69.

222 Courage Foundation, p 12.

223 News Media Association, p 4.

> The maximum sentence for secondary disclosers in the media, including journalists and editors should be no more than the current maximum of two years imprisonment. Sentences of above two years should also be precluded for primary disclosers adjudged to have disclosed the information in good faith and for a public interest reason to such a secondary discloser in the media.[224]

5.59 The National Union of Journalists argued that increased sentences would "exacerbate the chilling effect that official secrecy legislation has on public interest journalism".[225]

5.60 Mr Alan Rusbridger, former editor of The Guardian, made the following point:

> Having read a large proportion of the Snowden material and taken widespread advice I went ahead with publication, knowing I could face a jail sentence. The prospect of serving a longer period in jail would not in the least have deterred me.[226]

Classified evidence

5.61 We have been provided with evidence of the changing scope for damage owing to the developments in communication technology and bulk transfer/storage since the passage of the Act in 1989. As with all classified evidence, we are unable to publish it owing to its security classification, so the following is a hypothetical example that illustrates the risks revealed by the classified evidence:

(1) J, a contractor at GCHQ, downloads large volumes of material which she discloses to several major news organisations without assessing them for sensitivity or potential harmfulness. News organisation K publishes excerpts of the material based on internal legal advice and their own assessment of the consequences of publishing for UK interests. Organisation L publishes the entire cache of material in an un-redacted and searchable format. The information is accessed by foreign state actors and other subjects of interest who use it to target individuals identified as working for the UK, and also to protect themselves against the UK's intelligence gathering capabilities.

Analysis

5.62 Maximum sentences of more than two years' imprisonment have been imposed in the context of unauthorised disclosure offences in other legal systems, but we accept the point made by consultees that it is important to compare like with like. This is especially the case where other legal systems have different definitions, authorised disclosure procedures and defences.

5.63 Guardian News and Media and Liberty both submitted that the Canadian example was misleading, given the existence of a public interest defence in Canadian legislation. Although it is the case that Canada has a public interest defence, this only applies to sections 13 and 14 of the Security of Information Act 2001. Those offences concern the communication of safeguarded information or special operational information by persons who are "permanently bound to secrecy". Section 4 of the Security of

---

224 Associated Newspapers, para 7(e).

225 National Union of Journalists, p 32.

226 Alan Rusbridger, para 99.

Information Act 2001, which contains a broader unauthorised disclosure offence, is not accompanied by a public interest defence, but nevertheless carries a maximum sentence of 14 years' imprisonment.

5.64 Leaving the international comparison to one side, as we pointed out in our Consultation Paper, there are a number of unauthorised disclosure offences in English law which appear to be anomalous in terms of maximum sentence when compared with the offences contained in the OSA 1989. For example, a person who makes an unauthorised disclosure as specified under section 57 of the Investigatory Powers Act 2016 is, by virtue of section 59, guilty of a criminal offence. When tried on indictment the offence is punishable by up to five years' imprisonment and/or an unlimited fine.[227] This is very similar to the offence found in section 4(3)(a) of the OSA 1989, for which the maximum available sentence is two years' imprisonment and/or an unlimited fine. Whether the difference in maximum sentence between these two offences is rational must surely be open to doubt. We recognise that some stakeholders would argue that the maximum sentence for the offence contained in section 59 of the 2016 Act ought to be lowered to bring it into line with the offence in section 4(3)(a).

5.65 We do not consider that the maximum sentence for the offences contained in the OSA 1989 should be raised to 14 years' imprisonment. This would blur the distinction between the conduct criminalised by the OSA 1911 (espionage) and the conduct criminalised by the OSA 1989 (unauthorised disclosure). We accept that this distinction is important to retain.

5.66 We do, however, believe that there is merit in considering whether the maximum sentence in the OSA 1989 should be brought into line with the other unauthorised disclosure offences that exist in the criminal law of England and Wales. The aim would be to rationalise the maximum available sentences across all the unauthorised disclosure offences. Doing so would ensure that the maximum available sentences give the judge adequate sentencing powers in serious cases.

5.67 We also see force in the argument that the development of technology since 1989 has significantly increased the scope for damage flowing from an unauthorised disclosure (and, indeed, has changed the potential scale of unauthorised disclosures themselves). The evidence in this respect is striking.

5.68 As a number of consultees pointed out, the two-year maximum sentence also applies to those offences which can be committed by people other than Crown servants and government contractors. Should a review of the maximum sentences in the OSA 1989 be conducted, some consideration should be given to distinguishing the section 5 offence from the other OSA 1989 offences (not least because of the protection Article 10 of the European Convention on Human Rights affords those who are engaged in journalistic activity). This could either be achieved through a lower maximum sentence or through sentencing guidelines (for example, the section 5 offence could have a lower starting point). There is a cogent argument for saying that primary disclosures and secondary disclosures should not be equated for the purposes of maximum sentence.

---

[227] Soon to be repealed and replaced by section 59 of the Investigatory Powers Act 2016, which has the same penalties.

5.69 The Government Response discussed forfeiture of civil service pensions as a further possible sanction. Civil service pensions are automatically forfeited if the member is convicted of treason.[228] They may also be forfeited if the member is convicted of a "relevant offence". A relevant offence is defined as: (a) one or more offences under the OSA 1911 to 1989 for which the member has been sentenced to a term of imprisonment of at least 10 years' (which includes two or more consecutive terms of imprisonment which add up to at least 10 years); or, (b) an offence committed in connection with service as a public servant and in respect of which a Minister of the Crown has issued a forfeiture certificate. The Minister has the power to issue a forfeiture certificate where they consider that the members' offence "has been gravely injurious to the interests of the State or is liable to lead to serious loss of confidence in the public service".[229] We have concluded that this issue falls outside the scope of this project.

Recommendation 14.

5.70 A maximum sentence of two years' imprisonment does not provide the court with adequate powers in really serious cases.

5.71 Parliament should consider increased maximum sentences for some offences under the Official Secrets Act 1989.

5.72 Consideration should also be given to whether a distinction ought to be drawn in terms of maximum sentence between the offences in sections 1 to 4 of the Official Secrets Act 1989 and the offences in sections 5 to 6.

ACCESS TO LEGAL ADVICE

5.73 In our Consultation Paper, we noted the argument made by Alex Bailin QC that the OSA 1989 has the potential to interfere with an accused's unfettered right to instruct a legal adviser.[230] Section 13 of the OSA 1989 provides that:

> "disclose" and "disclosure", in relation to a document or other article, include parting with possession of it;

5.74 One consequence of this very broad definition is that a person suspected of an offence under the OSA 1989 may commit further offences when seeking legal advice on the alleged offence of which he or she is under suspicion. This is particularly relevant to the offence contrary to section 1(1) of the OSA 1989 as the offence is committed regardless of whether the disclosure is damaging.

5.75 The purpose of this chapter is to consider three broad questions:

---

228 Forfeiture Act 1870, s 2.

229 Public Service (Civil Servants and Others) Pensions Regulations 2014 (SI 2014/1964), Regulation 165(4).

230 CP, paras 3.190 to 3.196; A Bailin, "The Last Cold War Statute" [2008] *Criminal Law Review* 625, p 629.

(1) in what circumstances ought a disclosure of protected information to a legal adviser constitute an authorised disclosure for the purposes of the OSA 1989;

(2) are there further safeguards (such as personnel and premises vetting) that ought to be in place before that disclosure can be considered authorised; and

(3) what are the relevant Article 6 ECHR (right to a fair trial) considerations?

5.76 In our Consultation Paper we referred to *R v Shayler*,[231] in which Lord Bingham accepted that the right to a fair trial guaranteed in Article 6(1) of the European Convention on Human Rights ordinarily carried with it a right to seek independent legal advice. His lordship stated that this right could be satisfied by a member of the security and intelligence agencies seeking authorisation to disclose redacted information to a qualified lawyer or special advocate.[232] Lord Bingham was discussing the provision of legal advice in the context of a contemplated judicial review, however. He was not discussing the provision of legal advice in the context of criminal proceedings. The need for independent legal advice is more acute in the criminal context. We suggested that it could be considered contrary to principle to require the defendant to seek authorisation before he or she can seek legal advice.

5.77 The position in the official secrets context seemed anomalous when compared to other statutory regimes. For example, we noted that the Investigatory Powers Act 2016 states that a disclosure made to a legal professional for the purpose of receiving legal advice is an exempt disclosure for the purposes of that Act. We argued that a similar exemption could be provided in the OSA 1989 for a qualified legal adviser who was bound "to comply with any obligations that may be imposed upon them that relate to the need to safeguard information relating to the case". This might involve "vetting and security requirements".

5.78 It is important to understand what the security clearance and vetting processes seek to achieve. In respect of individuals, Parliament has stated that "the aim of security vetting is to ensure that the character and personal circumstances of an individual are such that he or she can be trusted with sensitive Government information or assets."[233] Having been through a vetting process would clearly serve to emphasise to the lawyer in receipt of the sensitive information what the consequences might be of unauthorised onward disclosure and failure to safeguard the information. A further value of the vetting process would be to allow the security services to assess the vulnerability of the lawyer to pressure from hostile agents to disclose the sensitive information.

5.79 However, vetting of individuals will be only one aspect of the vetting and security requirements. It is equally imperative that premises and IT systems offer sufficient protection of sensitive government data against hostile actors.

---

231 [2002] UKHL 11; [2003] 1 AC 247.

232 *R v Shayler* [2002] UKHL 11; [2003] 1 AC 247 at [34].

233 Houses of Parliament (2017) *National Security Vetting: Your Questions Answered,* available at https://www.parliament.uk/documents/PSD-Security-Vetting-booklet.pdf. This is also stated on the website for MI5, available at https://www.mi5.gov.uk/careers/vetting.

5.80 Of course, it is also important to recognise the practical implications of requiring vetting. Vetting and security requirements are expensive, time consuming and intrusive. Some lawyers would be unwilling to comply with the process even if at the state's expense. We have therefore considered whether the objectives of the vetting process can be achieved, albeit in diluted form, by strong professional obligations on legal advisers made via the relevant professional codes. We have concluded that they cannot.

5.81 Provisional conclusion 14 stated:

> A disclosure made to a professional legal adviser 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?

Consultation responses

5.82 The Institute of Employment Rights agreed that disclosure to a legal adviser should be exempt, but argued the law should go further:

> …limiting the [proposed] exemption to a barrister, solicitor or legal executive denies a potential whistleblower legal advice from whistleblowing organisations such as Public Concern at Work. Such organisations provide expert free advice as to the legal implications of a disclosure and can also advise an individual how to raise concerns internally to prevent the consequences of disclosure for all parties concerned.[234]

5.83 The Institute of Employment Rights suggested that placing vetting and security requirements on legal advisers may not be compliant with Article 6 of the European Convention on Human Rights.[235]

5.84 Dr Ashley Savage stated:

> This is an important addition which would remove current uncertainty. However, … there are several important considerations which must be explored … vetting may help to allay national security concerns, however there is a danger that individuals already concerned with the risks associated with making a disclosure will feel dissuaded from obtaining advice for fear that these vetted advisers are "part of the establishment". It is recommended that the policy arguments for and against vetting should be fully explored and the option of notification without vetting should be considered as an alternative.[236]

5.85 Peters and Peters stated:

> The right to seek legal advice, without being penalised for doing so, is a fundamental right which should be available to any individual who is the subject of a criminal

---

234 The Institute of Employment Rights, pp 21 to 22.

235 The Institute of Employment Rights, p 22.

236 Dr Ashley Savage, para 19.

investigation. Legal advisers are bound by legal professional privilege which, in any event, would prevent the onward transmission of the information to further third parties. The Law Society/Bar Council could be asked to issue guidelines on how legal advisers should maintain the information provided to them, for example, not storing the information on firm-wide computer databases.[237]

5.86 The Crown Prosecution Service agreed with our provisional conclusion but argued that the fact that a suspect may not be able to instruct the lawyer of their choice should not prevent a prosecution from taking place.[238]

5.87 The News Media Association stated:

> [The ability to make an exempt disclosure] must include the ability to seek pre-publication advice- which of course may lead to no publication specifically to avoid any commission of a criminal offence or damaging disclosure. Recipients of information such as the media may wish to avoid damaging disclosures, comply with the law and wish to seek advice internally from editorial and legal teams and externally from [the Defence and Security Media Advisory] Committee, external experts and external lawyers.[239]

5.88 Guardian News and Media agreed that disclosures to qualified legal advisers for the purpose of receiving legal advice in respect of an offence should be exempt, but they described the proposed vetting and security requirement as "deeply troubling".[240] Guardian News and Media raised specific concerns in relation to the position of journalists:

> However, where a journalist is concerned this would have serious repercussions if they were to discuss such matters with anyone else – an editor for example – there would still appear to be potential problems regarding the ability for offences to proliferate.[241]

5.89 The Bar Council and Criminal Bar Association joint response stated:

> A defendant must be able to give full instructions to his legal adviser. Whilst a special advocate can operate in discrete areas of evidence/disclosure in criminal proceedings, to deny a defendant proper access to his legal adviser may be in breach of ECHR Art 6(3)(c).
>
> The Bar Council has concerns about the suggestion that fully qualified legal advisers with current practising certificates ought to be subject to vetting before being given full access to the material on which to advise their clients … It is not clear whether it is proposed that there would be a panel of pre-vetted lawyers (to which exception may be taken) or a system whereby a suspect has a right to select a legal adviser of

---

237 Peters and Peters, p 9.

238 Crown Prosecution Service, p 6.

239 News Media Association, p 16. The Defence and Security Media Advisory ("DSMA") Notice system is discussed below, at 8.57.

240 Guardian News and Media, p 41.

241 Guardian News and Media, p 41.

his choice, subject to post-selection vetting. The latter course has the potential to result in considerable delay.[242]

5.90 Whistleblowers UK feared vetting and security might "prejudice the defence and could be open to abuse".[243] Individual consultee Damien Shannon also suggested that "only being able to instruct a lawyer approved by the very Security Service against one has, or may have, a legitimate grievance, creates an irreconcilable conflict of interest".[244] The BBC described the reference to "any vetting and security requirements as might be specified" as "concerning in that it suggests that there is potentially wide scope for undermining this principle".[245]

5.91 The Government Response stated:

> We agree subject to two caveats. First the exemption should apply only in relation to a person who has been arrested for or charged with an offence under the Official Secrets Act 1989 and for the purpose of them seeking advice and/or representation in relation to their arrest or prosecution. Secondly, the exemption should apply only if the legal adviser agrees to comply with such vetting and security requirements as may be specified and should cease to apply if the lawyer fails so to comply (in which case any security and intelligence material would need to be surrendered immediately to the originating authority).

Classified evidence

5.92 Following the government's response to our Consultation Paper, and in light of other responses on this point, we requested evidence from government to clarify the nature of the risk posed by handing sensitive material to independent lawyers. We have had sight of that evidence and, as with all secret or top secret evidence on which we rely, we include hypothetical examples that illustrate the risks revealed by that classified evidence:

(1) **Breach of security through inadequate systems in legal practice:** G, a lawyer, represents H, a civil servant seeking advice to understand the risk of prosecution under section 2 of the Official Secrets Act 1989 for leaking sensitive information regarding planned deployments in the Middle East via social media. G corresponds via email with H regarding the nature and content of H's unauthorised disclosure and H shares additional information, not included in the initial leak, which can be used to identify bases from which UK Special Forces are operating. Unbeknownst to G or H, G's email account has been compromised via a spear-phishing attack by a group affiliated with a foreign state, allowing them access to this information which is then used to target UK personnel. G also prints off this information as part of the case file. The office does not have suitable, security accredited, facilities to store or dispose of this material. Even if G is particularly security conscious there is a heightened risk of

---

242 The Bar Council and Criminal Bar Association, paras 48 to 49.

243 Whistleblowers UK, p 2.

244 Damien Shannon, p 3.

245 BBC, p 3.

this material being obtained by a hostile actor without G's knowledge and used to target UK personnel.

(2) **Exploitation of lawyers by foreign state actors – for example deliberate recruitment of lawyers who specialise in Hostile State Activity (HSA)**: A foreign state's intelligence services use other information gathered from G's email account (evidence of serious financial difficulties) to recruit him, and G is tasked to seek additional information from H in the context of preparing H's defence. H provides this information at G's request and the information is passed on to the foreign state's intelligence services where it's used to build a better understanding of the UK capabilities in the Middle East and plans for future engagement.

(3) **A corrupt lawyer using information provided to them by a client for personal gain**: Lawyer A is working with client B, a government contractor who has not been notified and is considering making a disclosure to the press about the details of a procurement which he is working on, as he considers it is being handled in an improper fashion. Lawyer A has, unbeknown to client B, close family and social connections to a foreign government. He advises client B that he should not under any circumstances make the disclosure, as this would be a serious offence. Having assured client B that he has destroyed the relevant materials, these are passed to an agent from the foreign government in return for a significant bribe to part of his family connected to the foreign government.

Analysis

5.94 This analysis section considers whether disclosures to legal advisers should be authorised disclosures for the purposes of the OSA 1989, and whether – in order for them to be so – particular safeguards need to be in place. Currently, a person who seeks legal advice, where doing so involves the disclosure of protected information, risks committing an offence under the OSA 1989. The need for someone to make such a disclosure may arise where they are suspected of an offence under the OSA 1989, but it is not limited to these cases. The problem arises wherever a person caught by the terms of the OSA 1989 might need to make a disclosure to a lawyer which involves disclosing information that might be protected by the OSA 1989. That could arise in investigations into misconduct in public office, and Official Secrets Act 1911 offences, among others.

5.95 It is worth briefly introducing the structure of this section. We begin with an analysis of Article 6 (the right to a fair trial), specifically as it relates to the right to access legal advice.

5.96 Following this, we consider two alternative scenarios in which protected material may need to be disclosed to a lawyer, and make recommendations accordingly.

(1) First, we consider whether disclosures to a legal adviser made prior to the commencement of a criminal investigation should be authorised (and, if so, with what safeguards in place). As we note, Article 6 ECHR does not apply in these scenarios, but the analysis is nonetheless different depending on whether the person is subject to section 1(1) OSA 1989 or one of the other OSA 1989 offences, and so we address these matters separately.

(2) Second, we consider whether disclosures to a legal adviser by a defendant or suspect in a criminal investigation should be authorised.

5.97 In resolving whether, in each of these scenarios, a disclosure of information within the scope of the OSA 1989 to the legal representative ought to be an authorised disclosure, a number of factors appear to be relevant:

(1) whether the disclosure is to a qualified lawyer: one authorised to practise in the UK and bound by the code of conduct of his or her profession;

(2) the legal obligations of the legal representative to whom the disclosure is made, and in particular any offences under the OSA 1989 which that person might commit by onward disclosure;

(3) whether imposition of some formal Government vetting or security clearance process for the lawyer is necessary or proportionate in order for a disclosure to them to be an authorised disclosure.

5.98 We conclude that legal advisers and their premises should be subject to National Security Vetting in order for a disclosure to be authorised, bearing in mind the otherwise unavoidable risk to national security. However, we do note that prosecution of those who make unauthorised disclosures to legal advisers could prove difficult: the defendant may be able, in certain circumstances, to demonstrate that he or she did not reasonably believe damage would result (where that is a requirement of the offence).

5.99 Overarching all of these issues is the requirement that the application of the OSA 1989 and any restriction it places on legal advice must be compatible with Article 6 of the European Convention on Human Rights ("ECHR"). We begin with that matter.

Article 6 considerations

5.100 As a number of consultees pointed out, restricting the pool of available legal advisers to those who have complied with vetting and security requirements potentially engages Article 6 of the ECHR. However, we are also conscious that the imperative to protect the information in question during an investigation for a suspected breach of the OSA 1989 can hardly be understated. The Government, as owner of the information, and the police and investigative agencies have a clear interest in minimising the risk of further dissemination. Disclosure to an unscrupulous or careless adviser, or to an adviser with inadequate data security systems, could cause as much harm, if not more, than the original loss of information. There is therefore a need to minimise this risk as far as possible, whilst also respecting the accused's rights under Article 6.

5.101 Given the strength of the views expressed by consultees, we believe it is important, in order to understand the arguments fully, to consider the extent to which any restrictions can lawfully under the Human Rights Act 1998 be placed on an individual's choice of legal adviser by, for example, requiring them to have some form of security clearance.

5.102 Article 6 states:

(1) In the determination of his civil rights and obligations or of any criminal charge against him, everyone is entitled to a fair and public hearing within a reasonable time by an independent and impartial tribunal established by law…

(3) Everyone charged with a criminal offence has the following minimum rights:

(a) […]

(b) […]

(c) to defend himself in person or through legal assistance of his own choosing or, if he has not sufficient means to pay for legal assistance, to be given it free when the interests of justice so require; …

5.103 "Charged with a criminal offence" has been interpreted broadly in domestic law. The editors of *Blackstone's Criminal Practice* note that: "… the right to legal assistance may apply prior to the decision to detain a person at a police station, and even before he has been formally arrested."[246] (See also paragraph 1.112.)

5.104 Any vetting and security requirements imposed upon lawyers who are privy to disclosures made by those subject to the OSA 1989, would need to be compatible with the defendant's right to "legal assistance of his own choosing".

5.105 The case law surrounding Article 6 has indicated that an individual's right to access a lawyer is not completely unfettered. For example, in *Brennan v United Kingdom*[247] the European Court of Human Rights ("ECtHR") held that the state may restrict access to a lawyer at the initial stage of a police investigation where there is good cause.[248] In that case, the police used section 45 of the Northern Ireland (Emergency Provisions) Act 1991 to defer a detained person's access to a solicitor for 24 hours. The ECtHR noted the Northern Ireland Court of Appeal's conclusion that the deferral was made in good faith and on reasonable grounds.[249]

5.106 Moreover, in *Re Maguire*,[250] a recent unanimous UK Supreme Court decision, the judgment of Lord Kerr emphasised the importance of achieving a fair trial and promoting the interests of justice.[251] Whilst the defendant's choice of counsel was to be taken into account, it was considered subordinate to these key aims.[252] The test

---

246 *Blackstone's Criminal Practice* (2019) at para D1.55.

247 (2002) 34 EHRR 507.

248 For a more detailed examination, see *Human Rights Law and Practice,* Lester, Pannick, Herberg (2009), at [4.6.70]

249 (2002) 34 EHRR 507 at [46 – 48]. Section 45 of the Northern Ireland (Emergency Provisions) Act 1991 is no longer in force, but similar provisions exist in section 58(6) to (10) of the Police and Criminal Evidence Act 1984 and Schedule 8 to the Terrorism Act 2000, paragraph 7A.

250 *In the matter of an application by Kevin Maguire for Judicial Review (Northern Ireland)* [2018] UKSC 17 (judgment given on 21 March 2018) ("Re Maguire").

251 *In the matter of an application by Kevin Maguire for Judicial Review (Northern Ireland)* [2018] UKSC 17 at [34].

252 *In the matter of an application by Kevin Maguire for Judicial Review (Northern Ireland)* [2018] UKSC 17 at [34].

was what the interests of justice require to ensure that an accused person is properly defended, rather than simply what his own particular wishes may be as to the manner of his defence.

5.107 Lord Kerr added:

> It is clear from this review of the relevant authorities that the essence of the right to choose one's counsel lies in the contribution that the exercise of that right makes to the achievement of the ultimate goal of a fair trial. It is not an autonomous right which falls to be considered outside that context.[253]
>
> … Article 6 does not invest an accused person with the right to demand that he have counsel of his choice at public expense, independently of the requirements of the interests of justice.[254]

5.108 These decisions and the interpretation of Article 6 suggest that it may be permissible under Article 6 to impose security and vetting requirements upon legal advisers to promote the interests of justice and assist the achievement of a fair trial. To ensure that any such vetting requirements are compatible with Article 6, it is important to create an overall system which maintains the defendant's trust in his or her representative and ensures the defendant is properly defended. The degree of vetting and security requirements to which lawyers could be subject would be key to determining whether such requirements are compatible with Article 6.

5.109 Our conclusion on Article 6 is therefore that some restriction on the freedom of those suspected of a criminal offence to choose any lawyer may be ECHR compatible.

5.110 We turn now to consider the two scenarios noted above to assess the extent to which any such restriction may be necessary. In addressing these scenarios, the issue we are seeking to resolve is whether a disclosure to a legal adviser, that would otherwise constitute an unauthorised disclosure under the OSA 1989, should be considered an *authorised* disclosure, and what further safeguards (if any) need to be in place in order for it to be so.

1. Legal advice sought by those not suspected of an offence

5.111 The position under consideration here is one where a person who is not subject to investigation or charge seeks legal advice, and doing so will involve making a disclosure of protected information to the lawyer. Since there is no live investigation, there is less opportunity for the State to regulate the type of legal adviser to whom the person turns for advice than would otherwise be the case; normally, upon the commencement of an investigation into a Crown servant, the State can (and does) provide legal assistance to that person.

5.112 In this context there are two important factors to have in mind. First, Article 6 applies to those subject to a criminal charge, and so would not apply prior to the criminal

---

253 *In the matter of an application by Kevin Maguire for Judicial Review (Northern Ireland)* [2018] UKSC 17, at [38].

254 *In the matter of an application by Kevin Maguire for Judicial Review (Northern Ireland)* [2018] UKSC 17, at [44].

charge. However, this term is wide in scope: the Strasbourg Court interprets "criminal charge" substantively, rather than formally, so would include "the official notification given to an individual by the competent authority of an allegation that he has committed a criminal offence".[255] This means it would apply to the initial stages of police interrogation.[256] Despite the breadth of "criminal charge", it is reasonably clear that Article 6 would not apply prior to this point. So, it would not apply to a person who was seeking legal advice about the consequences of making an unauthorised disclosure, nor where he or she has done so but is not yet a suspect.

5.113 Secondly, in practical terms, since the communication with the lawyer would be undertaken without notification to law enforcement agencies, there is no opportunity for the State to offer to provide clearance to the lawyers involved (assuming they did not already have the requisite clearance).

Those subject to section 1(1) OSA 1989.

5.114 Under section 1(1), the offence is committed without damage having been caused or even being likely. This offence can only be committed by current and former members of the security and intelligence services, and notified persons. In the event that such an individual made a disclosure to a lawyer for the purposes of seeking legal advice, the offence would be committed. That is so irrespective of the fact that the legal adviser to whom disclosure is made is both bound by professional obligations and would be at risk of committing other OSA 1989 offences (under section 5 of the OSA 1989) if he or she made an onward disclosure. It would also make no difference that the official had reasonable grounds to believe that the legal adviser would protect the confidentiality (so that the disclosure to him or her would not be damaging) and not further disclose (so no offence would be committed by the lawyer under section 5 OSA 1989).

5.115 We are not persuaded that it is necessary to provide authorisation for those working in the security and intelligence services (who know unequivocally that they are bound by section 1(1)) not to make disclosures in these circumstances). They are not suspects charged with an offence, and their legal position is clear to them. Further, there are numerous opportunities for such individuals to raise their concerns: with the Attorney General, Director of Public Prosecutions, Metropolitan Police Commissioner, Intelligence and Security Committee of Parliament, as well as with their Staff Counsellor or Ethical Counsellor (see below at **8.32**-**8.37**). Moreover, there would be a further and effective avenue for reporting concerns if our recommendation for a statutory commissioner in chapter 10 were to be implemented. We do not recommend that disclosure should be authorised in such circumstances and we are confident that that is compatible with Article 6 of the ECHR.

Those subject to offences under the OSA 1989 other than section 1(1)

5.116 In relation to sections 1(3) and 2-6 of the Act, it is not clear that the same considerations apply, or at least not to the same extent. The offences are slightly more complex than the section 1(1) offence, and there is greater scope for interpretation (for example, it may not be clear to the Crown servant or contractor whether a document

---

255 *Deweer v Belgium* [1980] ECHR 1, (1980) 2 EHRR 439 at [46].

256 *Ibrahim and Others v The United Kingdom* [2014] ECHR 1392, (2015) 61 EHRR 9 at [193].

relates to 'international relations' for the purposes of section 3). Whilst many Crown servants and contractors will know whether disclosure of material was liable to constitute an offence, and have access to a range of internal advice, it is clearly possible that a Crown servant or contractor may not know whether he or she falls within the scope of sections 1(3)-4 of the Official Secrets Act 1989 and may understandably wish to seek legal advice prior to being suspected of an offence. This is especially the case where he or she does not work regularly with sensitive material.

5.117 In any case, media consultees rightly highlighted the importance of journalists and editors – who might be subject to sections 5 and 6 – receiving pre-publication legal advice. (For ease of language, we distinguish "civilians" – ie those who are subject to section 5 and 6 of the OSA 1989 – from Crown servants, government contractors or notified persons. In practice, although sections 5 and 6 apply to civilians generally, they are of particular concern to the media and journalists).

5.118 Authorising a disclosure made for the purposes of obtaining legal advice can therefore be justified, so long as the risks of that disclosure can be managed. For the sake of protecting the sensitive information, a disclosure must only be lawful if there are safeguards in place. As we discuss below, these safeguards include not only the obligations to which lawyers are subject anyway (including professional obligations and the scope of the section 5 OSA 1989 offence), but also security of persons and premises.

5.119 Before we discuss those safeguards, it is worth noting that disclosure by a Crown servant or civilian to a lawyer for the purpose of legal advice will not invariably satisfy the elements of the offence because the defendant *may* be able to establish that he or she did not have reasonable cause to believe that the disclosure would be a "damaging" disclosure. This would obviously be context-dependent and would also depend on the knowledge of the defendant (which may be more sophisticated in the case of a Crown servant or expert journalist than in the case of a civilian), but we reach that conclusion on the basis that:

(1) the lawyer will be subject to professional obligations in relation to the information provided by a client for the purpose of obtaining legal advice (under the codes of conduct set by the Bar Standards Board for barristers or the Solicitors Regulation Authority: we deal with this is more detail below);

(2) the lawyer will be at risk of committing offences under section 5 of the OSA 1989 should he or she make further disclosures that are damaging (again, we consider this below); and

(3) therefore, the person making the disclosure may be able to rely on the belief that the disclosure to a qualified lawyer, under professional obligations, in these circumstances would not be damaging.

5.120 For the avoidance of doubt, we are not suggesting that professional obligations or the risk of criminalisation do in fact provide sufficient safeguards for protecting sensitive information. As we consider below, there are reasons and evidence to suspect that they do not. However, this is not to say that someone's *belief* that they provided effective safeguards would be wholly unreasonable, depending on their knowledge of the risks.

5.121 We now examine the safeguards more fully.

Lawyers' professional obligations

5.122 We consider that the professional obligations to which practising lawyers are subject provide an important (albeit limited) safeguard against onward disclosure. They are a necessary but not sufficient safeguard in respect of disclosures to legal advisers.

5.123 The Bar Standards Board sets core duties in its code of conduct, with which all practising barristers are obliged to comply. These include, for example, the duty to keep the affairs of each client confidential, act in the best interests of each client and act with honesty and integrity.[257] Similarly, in their code of conduct, the Solicitors Regulation Authority require practising solicitors to comply with certain principles, including acting with integrity, keeping the affairs of clients confidential, providing services to clients in a manner which protects their interests in their matter, subject to the proper administration of justice, and behaving in a way that maintains the trust the public places in them and in the provision of legal services.[258] Non-compliance with either of these codes of conduct can result in a finding of professional misconduct and lead to disqualification. Those who are not in regulated professions are not subject to professional obligations.

5.124 Having regard to the onerous nature of these obligations, and the fact that a breach of them in this context would be likely to be a career-ending step, we cannot agree with the Institute of Employment Rights' suggestion that disclosure to a "whistleblowing organisation" should also be authorised. If an individual at such an organisation, however defined, holds a current practising certificate, then a disclosure could be made to that individual (subject to further safeguards below), but we cannot recommend a general authorisation for any category of organisation.

5.125 We also disagree with the suggestion from Peters and Peters that legal advice privilege would be sufficient to protect sensitive material in this context. This is chiefly because legal advice privilege can be waived by the client (though there are further security considerations too). The client who is contemplating making an unauthorised disclosure should not be in a position to authorise further potentially damaging disclosures of protected government information.

5.126 We consider that there is merit in the relevant professional Codes being amended to emphasise to practitioners the nature of their obligations when providing advice in Official Secrets Acts contexts.

---

257 See Bar Standards Board Handbook, available at https://www.barstandardsboard.org.uk/regulatory-requirements/bsb-handbook/.

258 See Solicitors Regulation Authority Handbook, available at https://www.sra.org.uk/solicitors/handbook/pdfcentre.page.

Recommendation 15.

5.127 We recommend that the professional bodies responsible for the Codes of Conduct for practising lawyers – the SRA and BSB – consider including explicit guidance on the importance of maintaining confidentiality in cases involving the Official Secrets Acts, and the obligation not to receive disclosures unless they have the appropriate security clearance and premises assurance.

Offences for which the lawyer would be liable

5.128 Any legal adviser who receives information in confidence for the purpose of providing legal advice would be subject to section 5 of the OSA 1989.[259] For example, section 5(2) applies to information entrusted to an individual by a Crown servant or government contractor on terms requiring it to be held in confidence or in circumstances in which one could reasonably expect it to be so held.[260] Unauthorised disclosures by legal advisers of the protected information received in advising their client could therefore render the legal adviser subject to criminal liability under section 5 of the OSA 1989. That would apply as a necessary (but not sufficient) safeguard in relation to disclosure made to a legal adviser. Under such a threat of criminal liability for onward disclosure, we anticipate that any legal adviser would be even more cautious than normal in protecting the confidentiality of the material provided by the client.

5.129 We consider that the fact that prosecution under section 5 is possible is an important safeguard for the protected information. However, if this threat, coupled with the other safeguards we recommend, were not felt to be adequate in this context, the offence under section 8(1) could be extended. That section creates a summary offence where a Crown servant or government contractor fails to "take such care to prevent the unauthorised disclosure" of documents or articles to which the Act applies "as a person in his position may reasonably be expected to take".[261] One way to increase protection for the material in question would be to extend section 8(1) to apply to legal advisers who receive information for the purposes of providing legal advice.

5.130 We do not endorse Dr Ashley Savage's suggestion that legal advisers could be notified under section 1(6) of the OSA 1989. This is because, where a legal adviser was advising a client suspected of committing the offence contrary to section 1(3) of the OSA 1989, notifying the legal adviser would mean holding them to a higher standard than the client. It also fails to address some of the further risks that exist quite apart from the threat of criminal sanction.

---

259 We are not discussing the remote prospect of the lawyer being prosecuted for aiding and abetting the leaker, nor for liability under the Serious Crime Act 2007, Part 2.

260 Official Secrets Act 1989, s 5(1)(a)(ii).

261 Official Secrets Act 1989, s 8(1).

Security and vetting requirements

5.131 We deal first with the vetting of individuals. Despite the existence of these obligations and the threat of criminal sanction, there is nonetheless evidence that some lawyers have been exploited by foreign state actors, or corrupt, and have thus disclosed damaging sensitive information. We have noted hypothetical examples of this evidence above. It is also noteworthy that the professional obligations and threat of criminal sanction that attach to Crown servants and government contractors have not, in all cases, prevented the unauthorised disclosure of information. Vetting serves to reduce the risk of onward disclosure by managing the risk that an individual may be vulnerable to exploitation or motivated to disclose sensitive information.

5.132 Were this to be a required safeguard, any lawyer should be able to request National Security Vetting. In practice, someone seeking legal advice prior to their being suspected of an offence may, understandably, not wish to alert the State by having their lawyer request National Security Vetting. However, this problem is mitigated because a reasonable number of lawyers already hold security clearance (and this includes lawyers in private practice). The concerns that arise in the case of a criminal investigation (in which Article 6 is engaged) do not apply in this situation.

5.133 We turn to systems and premises security. None of the above safeguards provides assurance that a lawyer's information handling systems or premises are secure from interference. When government data is removed from government control, as it would be in the case where it is disclosed to a legal adviser, damage may well follow if it is not subject to similar levels of protection. Even the best intentions can be rendered entirely redundant if, as in the evidence noted above, a hostile actor can access the disclosed material. Worse, this can happen without the lawyer even being aware. Allowing protected material to be disclosed without equivalent levels of protection would render entirely vain the efforts and investment made to protect that material in the first place, and presents a real risk to national security. The information is only as safe as the weakest link in the chain permits it to be.

5.134 It is our view that the final safeguard must be systems and premises assurance by the government. We do not see that there is any way to circumvent this requirement, because even the most well-meaning and incorruptible lawyer may, unbeknown to them, present a security risk owing to the extent of their ability to retain information securely. In practice, this may not present a significant obstacle for lawyers, many of whom have sophisticated data-handling systems in place. However, the government is uniquely well-placed to understand the nature of the threat in respect of attempts to access official data, and is thus uniquely well-placed to check and provide advice in respect of data security.

5.135 **We therefore consider that a disclosure to a legal adviser by a Crown servant or government contractor not subject to section 1(1) OSA 1989 should, despite him or her not being a suspect in a criminal investigation, constitute an authorised disclosure subject to specific safeguards, which include professional obligations, security vetting and systems/premises assurance.** We do note, however, that any reasonable belief that damage would not result from the disclosure, whether or not damage was in fact likely, would pose an obstacle to prosecution.

Recommendation 16.

5.136 Where a person not subject to section 1(1) of the Official Secrets Act 1989 who is not a subject of a relevant criminal investigation makes a disclosure to a qualified lawyer for the purpose of obtaining legal advice, that disclosure should constitute an authorised disclosure, subject to specific safeguards being met.

5.137 The safeguards are as follows: (i) the legal adviser must be subject to professional obligations, either through the Bar Standards Board or the Solicitors Regulation Authority; and (ii) the lawyer to whom the disclosure is made must have undergone security vetting to the appropriate level and systems/premises assurance.

2. Legal advice sought when an investigation has commenced

5.138 We turn now to consider cases where the legal advice is sought by a person who is under suspicion of or charged with a criminal offence. The full rigour of Article 6 would apply in such cases.

5.139 We have already recommended that, subject to appropriate safeguards, a disclosure to a legal adviser would (save for those subject to section 1(1) OSA) constitute an authorised disclosure, whether or not they are a suspect in an investigation. The argument in favour of such a disclosure being authorised is yet stronger where a person is a suspect in a criminal investigation.

5.140 The law needs to provide for the appropriate access to legal advice in such situation, whilst respecting the need for confidentiality of the sensitive material. The safeguards already discussed would still have to apply – the professional obligations of the instructed lawyer coupled with adequate vetting/security (and the offences to which he or she would be subject). This would restrict the suspect's choice of lawyer, but we consider that it would be a restriction that is compatible with Article 6. This is because, as we discuss above, the aim of Article 6 is achieving a fair trial; a free choice of lawyer is important, but it is subordinated to that aim.

5.141 The question that arises in this scenario is whether a disclosure to legal advisers by those suspected of an offence under section 1(1) OSA 1989 should also constitute an authorised disclosure. As it stands, any disclosure to a legal adviser by a person subject to 1(1) would constitute an offence (and there is not even a requirement to prove likely damage or belief therein). It is clear that it should be an authorised disclosure, again subject to appropriate safeguards. The policy considerations that applied in the first scenario – that those subject to section 1(1) know that they are subject to it, and that there are many avenues for making authorised disclosures (especially if our recommendations for a statutory commissioner are accepted) – simply do not have the same force once a person is a suspect in an investigation, when Article 6 is engaged.

5.142 This position – that disclosures to legal advisers in this scenario should be authorised disclosures – was overwhelmingly supported by consultees. There was no unanimity on consultation on whether there should be a requirement for security clearance before such an exemption would apply. We note that the Government Response

contained the opinion that authorisation to disclose under the Act "should apply only if the legal adviser agrees to comply with such vetting and security requirements as may be specified". We also see considerable force in the Government's evidence that, regardless of the risks posed by the personal circumstances of the individual lawyer, inadequate systems and premises security can clearly pose a real risk to the security of the information.

5.143 For the purposes of the initial interviews in custody we consider that it would be legitimate for the legislation to mandate that the lawyer providing legal advice has to be one from lists of security cleared solicitors (that is, those who have undertaken a Security Check, the second highest level of National Security Vetting[262]).

5.144 In relation to the further stages of the investigation and any trial, we consider that the suspect should be offered the choice of any lawyer with relevant competencies from a list of those who already hold relevant security clearance. The suspect may well consider that it is worth having advice from such a lawyer who will not have to await clearance and who, given they have been cleared, already has some experience or expertise in the area.

5.145 In the event that the suspect prefers a lawyer who does not have security clearance, the lawyer would have the opportunity to obtain security vetting to the appropriate level and systems/premises assurance.

Recommendation 17.

5.146 We recommend that, where a Crown servant, government contractor or notified person is a suspect in a criminal investigation and makes a disclosure to a qualified legal adviser for the purposes of legal advice, that disclosure should be authorised for the purposes of sections 1-4 of the Official Secrets Act 1989 if the legal adviser has security clearance to the appropriate level, given the nature of the protected information, and has undergone systems/premises assurance.

PRIOR PUBLICATION

5.147 We noted in the Consultation Paper that there is currently no prior publication defence in the OSA 1989, although prior publication may in some cases have a bearing on whether a further disclosure is damaging. We agreed with the conclusion in the 1989 White Paper that second or subsequent disclosures may be more harmful than an initial disclosure, for example where an official confirms information that has been previously disclosed without lawful authority.[263] We provisionally considered that any

[262] Those with Security Check clearance are permitted frequent uncontrolled access to assets classified up to SECRET and occasional supervised access to TOP SECRET.

[263] Reform of Section 2 of the Official Secrets Act 1911 (1988) Cm 408, paras 62-64.

such defence should be limited to information "already lawfully in the public domain"[264] and widely disseminated.[265]

Provisional conclusion 15

5.148 Provisional conclusion 15 stated:

> 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 in the public domain and widely disseminated to the public. Do consultees agree?

Consultation responses

5.149 The BBC agreed with the provisional conclusion and did not object to "such a defence being limited to information which is lawfully in the public domain and widely disseminated to the public".[266]

5.150 The News Media Association considered the provisional defence of prior publication was:

> …too narrowly formulated, such that it could not be relied upon, even if all the world was already aware of the material disclosed and its disclosure had done no harm. Indeed, the consultative proposals would even criminalise the disclosure of information that could be lawfully released under the Freedom of Information Act.[267]

5.151 The News Media Association argued the proposal could give rise to satellite litigation on the meaning of lawfully and widely disseminated.[268] Guardian News and Media adopted a similar position regarding the terminology, and added that "a prior publication test is to be supported, but the test needs to be less stringent and more clear".[269]

5.152 The Bar Council and Criminal Bar Association described our provisional conclusion as "more restrictive than necessary". They were one of a number of consultees – including ITN[270] – who suggested the two parts of the test should be "either/or" rather than "and". They also suggested that that there should be a subjective element to the defence, such as belief on reasonable grounds that the prior publication was lawful or widely disseminated.[271]

---

264 A Bailin, "The last Cold War statute" (2008) *Criminal Law Review* 625, 629.

265 CP, paras 3.198 to 3.203.

266 BBC, p 4.

267 News Media Association, p 3.

268 News Media Association, p 12.

269 Guardian News and Media, p 63.

270 ITN, p 3.

271 The Bar Council and Criminal Bar Association, paras 50 to 54.

5.153 The Campaign for Freedom of Information and Article 19 joint response argued that the need for wide dissemination should be irrelevant if initial disclosure was lawful. They stated:

> We understand the concern that if there were *two* unauthorised leaks of the same information, a second widely disseminated leak might be more damaging than an initial unnoticed disclosure, and should not *automatically* benefit from a prior publication defence. However, if the initial disclosure is *lawful* this scenario is irrelevant.
>
> The Consultation Paper expressly recognises that a disclosure under the FOI Act would be such a lawful disclosure. Remarkably, it considers that this would not be sufficient and the information must also be widely disseminated.[272]

5.154 Associated Newspapers stated:

> There should be a defence of prior publication available in all the offences under the two pieces of legislation which can be charged against journalists and their sources. This should apply whenever the information in issue was already available to the public and the defence should not be restricted by a requirement that it became so lawfully.[273]

5.155 The National Union of Journalists made a similar point, and asked that we clarify the position where material is released lawfully under the Freedom of Information Act 2000.[274]

5.156 The Trinity Mirror agreed that a defence of prior publication should be included in the Act, but disagreed with the suggested approach:

> … it would have a huge chilling effect and would be disproportionate to prosecute a newspaper editor for following a story published by another publication using exactly the same information as originally published. If a newspaper followed up previous revelations but included new unlawful damaging revelations, then it could possibly be open to prosecute dependent on the individual circumstances, but to introduce the concept of a post publication gagging order would be contrary to article 10 of the European Convention on Human Rights and would, in any event, be unenforceable, given the amount of global news websites that would potentially follow the story.

5.157 The Crown Prosecution Service stated:

> If such a defence was raised the prosecution would need to show it was not lawfully in the public domain and widely disseminated. Dissemination is much easier and wider due to the internet and not always measurable. Mistakes can happen,

---

272 Campaign for Freedom of Information and Article 19, paras 41 to 42. Emphasis in original.

273 Associated Newspapers, para 7(d).

274 National Union of Journalists, p 17.

including announcements by Ministers/Ministries where the significance under OSA is not always appreciated.[275]

5.158 Peters and Peters noted the risk of over-criminalising the public, for example by criminalising retweets.[276] Dr Ashley Savage noted that consideration must be given to the meaning of "widely disseminated" in the light of "numerous methods of electronic communication and publication which are available".[277] Former intelligence officer, Annie Machon, queried how this provisional conclusion would operate in the internet age, in particular, asking how the phrase "widely disseminated" would be measured.

5.159 Oliver Butler objected on the basis that if the non-result model of drafting were adopted, prior publication should not be a defence as it would have no bearing on the culpability of an official if they did not know of it. He further submitted that the focus should be on whether further publication could do "more or fresh" damage. The good fortune of prior publication unknown to an official would not reduce culpability.[278]

5.160 The Government Response agreed with our provisional conclusion, subject to a series of caveats:

> It will be important to define with as much clarity as possible what is meant by the terms "widely disseminated" and "public domain". For example, we believe that information placed on a hard-to-find website, or published in a foreign language should not be regarded as "widely disseminated" for this purpose, even if the website or publication is in principle accessible by anyone. Further, the availability of information in the digital age can change over time: if it is widely accessible at one point but then becomes harder to find, may the information cease to be "widely disseminated" and if so, at what point? In a similar vein, what constitutes the "public domain" in the digital era? Is material shared by a social media group subject to privacy settings to be regarded as in the "public domain"? Does it depend on how large the group is and how strict or effective are the privacy settings? What is "the public" for these purposes?
>
> The law should make explicit that a previous disclosure will be lawful only if made in the course of official duty or pursuant to official authorisation.
>
> On a related point, the defence should not be available to someone who confirms or denies prior claims or allegations. For example, if the media speculate that a particular individual is a subject of MI5 investigation, and D publicly confirms this to be the case, D should not be able to claim the benefit of the defence by claiming that the media speculation constituted a lawful disclosure.
>
> The legal burden should rest on the defendant to prove that the information has been widely disseminated and that its disclosure was lawful. This is on the basis that it would be wrong for a person to disclose protected information without being sure it has been the subject of a prior lawful disclosure; and it is therefore reasonable to

---

275 Crown Prosecution Service, para 20.

276 Peters and Peters, p 9.

277 Dr Ashley Savage, para 22.

278 Oliver Butler, p 8.

expect them to evidence the facts that they say justify their actions. If a person chooses to disclose protected information without carrying out such due diligence, they should do so at risk that the disclosure is not within the scope of the defence.

Analysis

5.161 The relationship between damage and prior publication is currently an important one within the OSA 1989. Whether damage is caused by a particular disclosure will depend on a number of factors, including what other disclosures have been made, how far they have already been published, and their perceived credibility. As many consultees pointed out, the damage test in the OSA 1989 was intended to incorporate some consideration of prior publication. In our Consultation Paper, our aim was to ensure that a defence of prior publication would exist explicitly within the legislation. Given that in this Report we have recommended retaining the damage requirement in sections 5 and 6, this matter is not relevant as regards those sections. However, given that we recommend removing the damage requirement for the offences in sections 1(3) to 4, and there is no such requirement in section 1(1), further specific consideration needs to be given to whether there should be an explicit defence of prior publication.

5.162 A number of consultees raised questions as to the status of material which would be disclosable under the Freedom of Information Act 2000. We do not agree that if information that is encompassed by the OSA 1989 is *disclosable* (as opposed to having been disclosed) under the Freedom of Information Act 2000, its unauthorised disclosure would not constitute an offence under the OSA 1989 (or some other disclosure offence for information not subject to that Act). This is because the question of whether material is disclosable is only determined following an evaluation that is conducted by the owner of the information. There exists a number of grounds upon which the information may be exempt from disclosure. If the requester is dissatisfied with the decision to invoke an exemption he or she can appeal to the Information Commissioner's Office, the First Tier Tribunal, and can ultimately appeal through the civil court system. Similarly, the owner of the information can appeal a decision to order disclosure. This process has the capacity to deal with sensitive material. It would seem odd if a Crown servant could unilaterally pre-empt the comprehensive process created by the Freedom of Information Act 2000 by disclosing information without it having first been requested and without prior authorisation.

5.163 Information that has been *disclosed* following a freedom of information request is very different. As the Campaign for Freedom of Information and Article 19 rightly pointed out, material released pursuant to the Freedom of Information Act 2000 is considered to be in the public domain. Its disclosure would also be authorised. For the avoidance of doubt, we agree that these factors mean that no offence is committed by the further dissemination of information that falls into this category

5.164 Were a defence to be explicitly provided in a reformed OSA, one possible model defence upon which reliance could be placed is section 91.4 of the National Security Legislation Amendment (Espionage and Foreign Interference) Act 2018, which was recently enacted in Australia. Section 91.4(2) provides:

> It is a defence to a prosecution for an offence by a person against this [part of the Act] that the information or article the person deals with is information or an article

that has already been communicated or made available to the public with the authority of the [State].

5.165 We are not suggesting that this defence should be incorporated wholesale into English law. For example, the provision would need to be tailored to apply to Crown servants and also to ensure that it does not undermine the operation of any current legislation, such as the Freedom of Information Act 2000. We consider that a provision similar to this one in English law would address the concerns which were expressed by those consultees who represent the media.

5.166 This provision does not, however, address the further contention that the mere fact of information being in the public renders subsequent disclosure harmless. We agree that subsequent disclosure may, in certain circumstances, be as or more damaging than the first. We also recognise, however, that "widely disseminated", as a proxy for whether or not subsequent disclosure would be damaging, is not easy to measure. We also see little benefit in framing the defence around whether the subsequent disclosure was damaging. Not only would this resurrect problems of proof and policy discussed in the preceding chapter, but it would also make the success of the defence very hard to predict before the fact, even in the case of widely-disseminated information.

5.167 Instead, we are of the view that the first limb of the test (that the information in question was in fact already in the public domain) should, if drafted appropriately, achieve what is required. If the defendant can demonstrate that the information has been communicated *to the public* – rather than merely to a small fraction thereof (for example, by having been posted to a website with no views, or shared with only a couple of people), then many of the concerns raised by consultees will be met.

5.168 Where we recommend that the offences in the OSA 1989 retain the requirement to prove damage (ie sections 5 and 6), one way to incorporate prior publication into the legislative scheme is to make clear that where there is evidence of prior publication this is a factor that is relevant to whether the disclosure was damaging. This would ensure that what is currently implicit within the legislative scheme is made explicit. The other offences would not contain a damage requirement, and section 1(1) of the OSA 1989 contains no damage requirement anyway, so this analysis does not apply. One way to incorporate the question of prior publication into this offence is to enact a provision that is quite similar to the one contained in section 91.4(2) of the Australian Act. The consequence of doing so is that it would not be an offence for a member of the security and intelligence agencies or a notified person to communicate information that has already been communicated to the public or made available to the public with lawful authority. This would apply, for example, to information that has been disclosed under the Freedom of Information Act 2000.

Recommendation 18.

5.169 It should be made explicit that prior publication is a factor that ought to be considered by prosecution agencies, courts, and juries when determining whether an unauthorised disclosure was damaging for the purposes of the sections 5 and 6 offences under the OSA 1989.

5.170 It should be made clear that it is not an offence for the purposes of sections 1(3) to 4 to communicate information that has been already communicated to the public or made available to the public with lawful authority.

CATEGORIES OF PROTECTED INFORMATION

5.171 In our Consultation Paper, we noted that some commentators have argued that the categories of information encompassed by the OSA 1989 are too broad. We cited commentary that described section 3 (international relations) as "troublingly wide".[279] We noted that we had received no evidence to substantiate those views, but welcomed consultees' views on this point.

Consultation question 8

5.172 Consultation question 8 stated:

> 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 responses

5.173 The Crown Prosecution Service did not suggest any amendment to limit the existing categories.[280] Neither did the Government Response, which stated:

> The 1989 Act was very effective in narrowing the protection of the law to information properly regarded as sensitive and the Government sees no case for drawing the categories of protected information more narrowly than they already are.

5.174 The Government Response disagreed with the suggestion in our Consultation Paper that the definition of "international relations", the category protected by section 3 of the OSA 1989, is "troublingly wide". The Government Response gave a number of examples where information relating to international relations is excluded from court proceedings. These include, for example, rule 4(1) of the Special Immigration Appeals Commission (Procedure) Rules 2003, which requires the Commission to secure that information is not disclosed contrary to the international relations of the UK, amongst others, and rule 80.2(2) of the Civil Procedure Rules (information must not be disclosed contrary to the public interest).

---

279 See G Robertson, *Freedom, the Individual and the Law* (1993), pp 168 to 173.

280 Crown Prosecution Service, p 6.

5.175 A significant number of consultees submitted that the categories encompassed by the legislation are too broad.[281] English PEN/Index on Censorship/Reporters Without Borders argued that a broader scope would be regressive. Instead, there was a need to "provide for more precisely-defined categories of protected information".[282]

5.176 The News Media Association stated:

> The categories of information protected by the OSA 1989 are widely drawn. However, the Act's deliberate focus upon 'damaging' disclosure help to avoid undue restrictions upon freedom of expression. Narrowing the categories would not counteract the chilling effect of the Law Commission's other proposals. In any event, even if the OSA were otherwise unchanged, any change to the categories would have to be carefully analysed to ensure that the intended 'narrowing' did not create new problems of legal uncertainty or inadvertently increase the potential for prosecution of journalists.[283]

5.177 The Institute of Employment Rights stated:

> …the disclosure of *any* information, document or other article relating to defence in section 2 or *any* information, document or other article relating to international relations in section 3 is far too broad. These categories of information are very widely drafted and such broad definitions are particularly problematic if the element of damage is removed from the offence.[284]

5.178 Liberty stated:

> As we urged the Government during the Parliamentary passage of the Investigatory Powers Bill, we urge that the Law Commission to adopt a significantly tighter, clearer, and less abuse-prone definition of national security, drawing on the definition of national security provided by UN's Siracusa Principles. It lays down a standard that 'national security' may only be invoked to protect "the existence of the nation or its territorial integrity or political independence against force or threat of force." This would ensure that national security remains tightly defined, permitting official secrecy only where truly justified.[285]

5.179 The BBC stated that it "did not support any proposal which would result in a significant broadening of the protected categories of information."[286]

5.180 Oliver Butler argued that for officials, wide categories of information were more acceptable if the offence was limited to culpable unauthorised disclosures and reasonable belief in capacity for damage. He was not persuaded, however, that private individuals should owe similar duties where they come into possession of

---

281 Peters and Peters, p 10; Dr Ashley Savage, p 8; News Media Association, p 17; The Institute of Employment Rights, p 23.

282 English PEN, Index on Censorship and Reporters Without Borders, para 73.

283 News Media Association, p 17.

284 The Institute of Employment Rights, p 20. Emphasis in original.

285 Liberty, para 64.

286 BBC, p xxx.

information, such as information on international relations. The basis for this was his view that "the duties owed by private individuals should not be as extensive as those owed by officials". Mr Butler also noted that the potential side effect of narrowing the categories of information might be a proliferation of specific disclosure offences, as occurred following the replacement of section 2 of the 1911 Act with the OSA 1989.[287]

5.181 Dr Ashley Savage stated that he:

> … believes that more consideration needs to be given to the drafting of the categories of information encompassed by the Official Secrets Act 1989. As the Law Commission will be aware, several academic and professional authors have argued (over the course of several years) that the categories are overly broad. It is submitted that these views have merit. It is perhaps not that these broadly drafted categories are resulting in a large number of convictions, as the author has previously stated in his own work on this area, the number of prosecutions (where this information has been made available) is very small. However, the impact of arrest and potential loss of security clearance must be considered together with the application of the Official Secrets Act 1989. To the best of the author's knowledge there is little information on the number of arrests carried out for Official Secrets Act offences. However, *Stankovic v Chief Constable of Ministry of Defence Police* illustrates the potential difficulty. In that case, a Major in the British Army was arrested for offences under the Official Secrets Act 1989. The episode took over two years to resolve and ultimately no charges were brought but Stankovic had lost his security clearance.

5.182 Dr Savage suggested that section 3(6) of the OSA 1989 was particularly vague as it referred to "confidential" documents, whereas the Government Security Classification Scheme does not include such a classification.[288]

Analysis

5.183 A significant number of consultees expressed the view that the categories of information encompassed by the OSA 1989 are too wide. Consultees did not provide us with guidance as to how the categories could be more narrowly drawn, however. Helpfully, Liberty did remind us of the Siracusa Principles.[289] The Siracusa Principles on the Limitation and Derogation of Provisions in the International Covenant on Civil and Political Rights were published in 1985 by the United Nations Economic and Social Council. As Liberty pointed out, they refer to the term "national security". As we discussed in Chapter 3 (at 3.44, for example), this was not a term which consultees thought appropriate for use in the context of the Official Secrets Act 1911. Whether the categories of information that are currently encompassed by the OSA 1989 ought to be replaced with a single category of information relating to "national security" is certainly one option. Doing so may give rise to difficulties of interpretation, however, unless the concept of "national security" is further defined. Whilst there is a partial

---

287 Butler, p 8.

288 Savage, p 8.

289 See: United Nations, Economic and Social Council, Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights, U.N. Doc. E/CN.4/1985/4, Annex (1985), available at http://hrlibrary.umn.edu/instree/siracusaprinciples.html.

definition in the Siracusa Principles, it is very narrow and is probably narrower than how the concept "national security" is typically understood in domestic law. Furthermore, the term would not encompass information that currently falls within section 4 of the OSA 1989, which relates to, amongst other things, information that facilitates an escape from legal custody. Whether it should no longer be a criminal offence to disclose without lawful authority information that falls into this category is a question that would require detailed consideration.

5.184 A majority of consultees expressed the view that the categories of information currently encompassed by the OSA 1989 ought to be narrowed. Despite the sincerity of the views that were expressed, we have little guidance to assist us in how we would achieve this aim. For this reason, we have concluded that the categories should, at this time, remain as they are. For any reform of the OSA 1989, however, the possibility of defining the categories of information with greater precision is a matter that ought to be explored as a priority.

Recommendation 19.

5.185 The categories of information currently protected by the Official Secrets Act 1989 should not be narrowed at this time. For any reform of the Official Secrets Act 1989, however, the possibility of defining the categories of information with greater precision ought to be explored as a priority.

SENSITIVE ECONOMIC INFORMATION

5.186 In our Consultation Paper we suggested that extending the categories of protected information to encompass sensitive economic information "merits further consideration". We suggested the definition of information that affects the economic well-being of the United Kingdom in so far as it relates to national security, a model found in the Investigatory Powers Act 2016, might be used.[290] This was not a provisional conclusion, but was merely a consultation question and we invited consultees' views on it.

5.187 Consultation question 9 asked:

> 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?

Consultation responses

5.188 The Crown Prosecution Service stated that the extension "makes sense" and questioned whether it should be limited to information "in so far as it relates to national security".[291]

---

290 CP, paras 3.210 to 3.213.

291 Crown Prosecution Service, p 7.

5.189 Similarly, the Government Response stated:

> We consider that information relevant to the UK's economic well-being is covered by the spying offence in the Official Secrets Act 1911 and should remain covered by a reformed law of espionage, on the basis that this is in the interests of the UK. It would seem inconsistent for such information not also to be protected by the Official Secrets Act 1989.

5.190 The majority of consultees objected in the strongest possible terms to any expansion. It is fair to say that this was one of the most controversial consultation questions in our paper.

5.191 Associated Newspapers argued that our definition was insufficiently precise to merit criminal liability. They questioned our analogy with the Investigatory Powers Act 2016, noting that the purpose of that legislation was to permit a means of investigation, not to create criminal liability. In relation to the effect on journalism, ANL stated:

> [We] would be particularly concerned if any class of information of this sort were included in the legislation, without a public interest defence in the relevant offence, given how much legitimate public interest journalism is based on official information about the economy.[292]

5.192 News Group Newspapers also questioned the analogy with the Investigatory Powers Act 2016:

> The IPA primarily involves a limitation of rights under Article 8(1) of the European Convention on Human Rights (ECHR), and Article 8(2) allows for this *"in the interests of … the economic well-being of the country."* By contrast, the Official Secrets Act primarily involves a limitation of rights under Article 10(1) of the ECHR, but Article 10(2) does not contain an express *"economic well-being"* justification.[293]

5.193 In their joint response, English PEN, Index on Censorship and Reporters Without Borders were highly critical of this consultation question:

> 'Economic information,' is an overbroad category; '[A]s it relates to national security' only marginally less so. The Act lacks interpretive clarity in regard to the parameters of the 'national interest.' The generic formulation put forward in the Consultation Paper – 'sensitive information relating to the economy in so far as it relates to national security' – would do little, if anything, to resolve this ambiguity; it is just as likely, if not more, that it would compound the problem.[294]

---

292 Associated Newspapers, para 29.

293 News Group Newspapers, para 15. Emphasis in original.

294 English PEN, Index on Censorship, Reporters Without Borders, para 74.

5.194 English PEN, Index on Censorship and Reporters Without Borders were among a number of consultees who argued that a similar point had been considered and rejected by the Franks Committee in 1972.[295] Further, they stated:

> A further problem inherent in the lack of specificity as to the language and content of the proposed category is revealed by a hypothetical scenario in which a Crown agent unlawfully discloses information which carries the potential to cause grave harm to the national economy but that, for whatever reason, this harm or damage does not come to pass. Would such a situation violate the protected category in the manner of a strict liability offence, on the basis of conduct alone? Or would the offence only be engaged in the case of damage arising as consequence of the disclosure? If the former, the offence would be so broad as to criminalize most, if not all, legitimate disclosures. If the latter, however, the category would fail in its purpose in that it would not carry the same deterrent force.[296]

5.195 Dr Ashley Savage stated:

> Without further evidence to justify the need for this section it is difficult to see why it should be introduced. [I am] … concerned that its inclusion, without a clear and well evidenced justification, would present an unnecessary retrograde step. The 1989 Act was aimed at narrowing the circumstances where individuals could be prosecuted. As previously discussed, the author (and many others) have suggested that the drafting of the current sections is too wide. It is difficult to consider how economic information protected under 'national security' grounds may be included without it resulting in broad and uncertain application.[297]

5.196 The Courage Foundation were similarly critical of the term "economic well-being so far as it relates to national security" as it features in the Investigatory Powers Act 2016.[298] They cited the Intelligence and Security Committee of Parliament's report on the Draft Investigatory Powers Bill 2016, which described the term as "unnecessarily confusing and complicated":

> …if 'national security' is sufficient in itself, then "economic well-being… so far as [is] relevant to the interests of national security" is redundant, since it is a subset of the former. We have questioned both the Agencies and the Home Office on this matter and neither have provided any sensible explanation. In our opinion, this area is already sufficiently complex so drafters should seek to minimise confusion wherever possible. We therefore recommend that 'economic well-being' is removed as a separate category.[299]

5.197 Public Concern at Work stated:

---

295 UK Open Government Network, p 3; Public Concern at Work, p 2; Courage Foundation, p 13; Liberty, p 21; and Guardian News and Media, p 63.

296 English PEN, Index on Censorship, Reporters Without Borders, para 76.

297 Dr Ashley Savage, para 25.

298 Courage Foundation, pp 11 to 12.

299 Intelligence and Security Committee, Report on the Draft Investigatory Powers Bill (9 February 2016), HC795, p 10.

> We are not convinced that there is sufficient justification in the Law Commission report for such a dramatic and far reaching reform to the OSA.
>
> The disclosure or improper use of market sensitive information is already criminalised through other parts of criminal law e.g. insider trading etc... With this in mind we are unsure what criminal act this extension would be outlawing.
>
> Our fear is that it will be used to hide Government embarrassment behind the facade of national security. For example, should a concerned civil servant who discloses to the press controversial details on a trade negotiation, or the state of affairs during the Brexit negotiations really be criminally liable for such triggering a public debate? Should the journalist in receipt of such information be concerned that they could fall foul of the OSA. We also fear a chilling effect on public debate where Government experts and officials will feel they need to be more careful about their public comments about the effect of Brexit or any other economic event in fear that it will fall foul of the OSA.[300]

5.198 Global Witness called it "one of the most dangerous proposals" and expressed concern that it could result in the suppression of embarrassing or inconvenient information by Government.[301] Compassion in Care argued that economic damage "could be misused by the state to protect the corporate interests of private companies to the degree that any damaging information could be suppressed for fear of prosecution".[302]

5.199 Individual consultee Chris O'Donovan suggested that the "economic well being of the UK, in so far as it relates to national security requires a tighter definition".[303] Douglas Green suggested that it would mean the concept of "national security" would be "widened to an unnecessary degree which goes well beyond what a reasonable person would believe to be genuine security considerations".[304]

5.200 Liberty stated:

> We are extremely concerned that such a change would permit Government to cloak all manner of information with the veil of secrecy, including information that has no national security impact whatsoever.[305]

5.201 The News Media Association and Guardian News and Media were concerned that budget leaks, Brexit negotiations, international trade negotiations, views on NATO spending, and exchange rates could be covered.[306] The National Union of Journalists wanted "absolute assurances that the definition of economic well-being could not be

---

300 Public Concern at Work, paras 18 to 20; Liberty, p 21.

301 Global Witness, by email.

302 Compassion in Care, p 2.

303 Chris O'Donovan, by email.

304 Douglas Green, by email.

305 Liberty, para 59.

306 News Media Association, p 17; Guardian News and Media, pp 2, and 64 to 65.

used in relation to information, material and/or data linked to the legitimate activities of trade unionists and trade unions."[307]

5.202 Peters and Peters stated:

> Disclosures of information concerning large corporations such as banks (for example at the time of the 2008 financial crisis) could have a harmful effect on the UK economy but, in our view, should not be criminalised. The aim of this legislation is not to protect corporate interests. The public's perception and support for the Act is important. An average person may find it difficult to consider the leaking of economic information as espionage, as understood in the strictest sense.[308]

Analysis

5.203 As set out above, the vast majority of consultees strongly objected to expanding the categories of information encompassed by the OSA 1989 to include economic information in so far as it relates to national security. We agree with News Group Newspapers to the extent that the analogy to the Investigatory Powers Act 2016 is not a perfect one.

5.204 Criminalising the unauthorised disclosure of economic information in so far as it relates to national security could perhaps be justified under the "in the interests of national security" and/or the "preventing the disclosure of information received in confidence" qualifications contained in Article 10(2) of the European Convention on Human Rights. Whilst we note the argument advanced by the Government Response, we do not consider that the case for an expansion of the categories in the OSA 1989 has been made out. We have been particularly influenced by the responses to the previous consultation question and the fact that so many consultees expressed concerns about the breadth of the categories which are currently encompassed by the OSA 1989.

Recommendation 20.

5.205 The categories of information protected by the Official Secrets Act 1989 should not be expanded to include economic information in so far as it relates to national security.

EXTRATERRITORIALITY

5.206 In our Consultation Paper we considered the extraterritoriality of the offences contained in the OSA 1989. We noted how the legislation currently applies abroad to encompass Crown servants and government contractors who are British citizens. We noted, however, that a person who is not a British citizen or Crown servant does not commit an offence if they disclose the information outside the UK. This is true even if they are a "notified person", as defined in section 1 of the OSA 1989. We asked

---

307 National Union of Journalists, p 3.

308 Peters and Peters, p 10.

consultees for their views on the extent to which this creates a gap in the protection the legislation affords sensitive information. Some consultation responses appeared to be based on a misunderstanding of our position: we were not advocating for an expansion of the categories of person to include those who were not Crown servants, government contractors or notified persons.

Provisional conclusion 16

5.207 Provisional conclusion 16 stated:

> 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 UK and irrespective of whether the Crown servant, government contractor or notified person who disclosed the information was a British citizen. Do consultees agree?

Consultation responses

5.208 The Crown Prosecution Service agreed, as did the Government Response, which stated:

> We agree with this provisional conclusion as damage may be caused regardless of who makes the disclosure and where it takes place, especially in an internet-enabled world.

5.209 Dr Ashley Savage agreed, as did Peters and Peters, who stated:

> If the person making the disclosure threatening UK interests is not a British citizen and he makes that disclosure outside of the UK, there is no reason why he should not be prosecuted if all the required elements of the offence are present. As discussed in the context of the offence of espionage, state borders are now less significant when it comes to information storage than was the case prior to the digital era. It is easy to send information worldwide with the push of a button. The protection afforded to sensitive information must therefore be enhanced to meet this new challenge.[309]

5.210 The Bar Council and Criminal Bar Association stated:

> There is force in the proposition in principle. As with the 1911 Act offences (Provisional Question 7), the extent of the required links will need to be considered, whether on a 'last act' or 'substantial measures' basis.[310]

5.211 The Courage Foundation questioned the practicality of extending territoriality, and also expressed concern about the potential effect on journalists:

> New extraterritorial provisions would appear to significantly broaden the scope of the offences from British officers and subjects to those with a "significant link" to the UK.

---

309 Peters and Peters, p 10.

310 The Bar Council and Criminal Bar Association, para 57.

> The Report refers to the 2015 amendments of the Computer Misuse Act, which uses the same term "applied in various ways". It is unclear what a "significant link" might mean in practice and whether the Commission is proposing that foreign journalists, for instance, might face prosecution if they published information that falls into a category protected by the Official Secrets Act.
>
> If this is indeed what the Commission is proposing, it is unclear whether thought has been given to the likely possibility of foreign nationals being extradited to face charges of this type in the UK, particularly given the French courts' refusal to extradite David Shayler in 1998.
>
> Not only does it undermine the principle of deterrence if laws are unenforceable, the assertion of extraterritorial jurisdiction raises the possibility of states trying to enforce reciprocal laws against UK.[311]

5.212 Guardian News and Media stated:

> Assuming the extended jurisdiction could also apply to a recipient of information such as a journalist this may also expand the scope for prosecutions of such individuals.[312]

5.213 The National Union of Journalists stated:

> There should be limits on the use of any new extra-territorial offences in regard to journalists and media organisations abroad.[313]

Classified evidence

5.214 We have seen classified evidence of damaging behaviour that is not currently criminalised owing to the extraterritoriality provisions in the OSA 1989. The following is a hypothetical example that illustrates the risks revealed by the classified evidence (though, as we note in our analysis below, our OSA 1989 recommendations would not criminalise F in this example – albeit that he might be guilty of an espionage offence under the OSA 1911):

(1) E, a UK national and Crown servant, discloses sensitive information relating to a trade agreement with an allied state to F, a foreign national living outside the UK. F operates a website which invites government employees to disclose sensitive information in the name of transparency and publishes this information with no questions asked. The publication of the information damages relations with the allied state and has a detrimental impact on negotiations. The UK authorities are unable to prosecute F for his role in the damage caused if he subsequently travels to the UK.

---

311 The Courage Foundation, p 12.

312 Guardian News and Media, p 65.

313 National Union of Journalists, p 3.

Analysis

5.215 The issue that was being discussed in this part of our Consultation Paper was a narrow one: aside from the territorial ambit of the offence, we were concerned to ensure that the offence applied equally to government contractors and notified persons (whether or not they were British citizens) as it did to British citizens and Crown servants. We did not consult on expanding the categories of person to include foreign citizens who were not also Crown servants, government contractors or notified persons.

5.216 By virtue of section 15(1) the offences in the OSA 1989 can be committed when a British citizen or Crown servant is abroad. Section 15(1) provides:

> 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.

5.217 As Professor Michael Hirst points out, this is sensible, as it would be anomalous for sensitive information to lose the protection of the criminal law just because the person who possesses it happens to be outside the United Kingdom.[314]

5.218 As we have already explained, the OSA 1989 is unusual. Unlike the vast majority of Acts of Parliament, an individual is not subject to its provisions simply by virtue of being within the jurisdiction of the United Kingdom. To be subject to sections 1 to 4 of the OSA 1989, an individual must be a Crown servant, government contractor, or notified person. If an individual is a Crown servant, or a British citizen, and discloses information without lawful authority while abroad, he or she will commit a criminal offence. In the discussion in the Consultation Paper, we were considering the criminal liability of someone who is not a British citizen, but who may be a government contractor or a notified person, and who discloses information while abroad, without lawful authority. That person does not currently appear to commit a criminal offence. We were asking consultees for their views on whether this gap is anomalous and ought to be closed.

5.219 We agree with Dr Ashley Savage that, "if the person making the disclosure threatening UK interests is not a British citizen and he makes that disclosure outside of the UK, there is no reason why he should not be prosecuted if all the required elements of the offence are present". Our goal is to ensure that those who are already subject to the legislation remain so when they are outside the United Kingdom.

5.220 The example of the evidence cited above would not fall within the scope of our provisional conclusion in the Consultation Paper. We do see the force in the argument

---

314 See generally: M Hirst, *Jurisdiction and the Ambit of the Criminal Law* (2003).

that there might be circumstances such as these in which damaging, unauthorised disclosures ought perhaps to be prosecuted. It is worth noting that certain disclosures may be caught by the espionage offence contained in the Official Secrets Act 1911 (espionage by communication of information), subject also to the requisite intent and extraterritoriality provisions. Nonetheless, as our provisional conclusion did not specifically address this point, we make no recommendation in this respect.

5.221 Sections 1-4 will continue to apply only to those to whom they already apply in the UK. However, we are recommending that the legislation apply to those people – Crown servants, government contractors and notified persons – regardless of whether they commit the offence in the UK and irrespective of whether they are British citizens.

Recommendation 21.

5.222 The territorial ambit of sections 1 to 4 of the Official Secrets Act 1989 should be amended so that a government contractor or notified person commits an offence when he or she makes an unauthorised disclosure abroad irrespective of whether he or she is a British citizen.

OPTIMAL LEGISLATIVE VEHICLE FOR REFORM

5.223 In our Consultation Paper we expressed the view that it would be undesirable to attempt to remedy the problems with the current law by amending the existing legislation. We suggested that the title of the Official Secrets Act did not accurately convey its purpose or make enough of a distinction between the conduct that is criminalised by the Official Secrets Acts 1911-39 and the Official Secrets Act 1989. We also pointed to practical reasons such as ease of redrafting for preferring a new Act over amending the existing law.[315]

Provisional conclusion 17

5.224 Provisional conclusion 17 stated:

> The Official Secrets Act 1989 ought to be repealed and replaced with new legislation. Do consultees agree?

Consultation responses

5.225 Several consultees welcomed this proposal.[316] The Crown Prosecution Service welcomed the opportunity to close loopholes and amend sentencing and notification provisions.[317] Peters and Peters argued that a "clean slate", a "higher degree of clarity" and a more accurate title were required.[318] Dr Ashley Savage commented that

---

315 CP, paras 3.227 to 3.230.

316 The Bar Council and Criminal Bar Association, p 11; Whistleblowers UK, p 3; Oliver Butler, p 8.

317 Crown Prosecution Service, p 7.

318 Peters and Peters, p 11.

OSA 1989 is "outdated and no longer fit for purpose",[319] while the Institute of Employment Rights cautioned that it was "just a change of title unless it enacts real reform".[320]

5.226 The Government Response stated:

> We have no settled view on whether the existing law should, Parliamentary time permitting, be amended or repealed and replaced by a fresh statute. We agree that the title of any new statute should reflect that its object is to protect official information from unauthorised disclosure, e.g. the "Protection of Official Information Act".

5.227 A significant number of consultees were worried that any new statute would be used to increase the amount of information that is encompassed by the criminal law and would further restrict freedom of expression, a right guaranteed by Article 10 of the European Convention on Human Rights and the special protection afforded to that right by section 12 of the Human Rights Act 1998.

Analysis

5.228 We continue to believe that there is merit in an entirely new statute. In particular, we take the view that the statute would benefit from a name that more accurately reflects what it is trying to achieve – such as the Protection of Official Information Act. This would need to be achieved by a new Act of Parliament. This would not just be a superficial change, as a new Act of Parliament would enable a public debate to take place around some of the concerns which stakeholders brought to our attention. We envisage that this would include, but would not be limited to, the question of whether the categories of information currently encompassed by the legislation are too broad and whether they can be more precisely defined.

5.229 We continue to believe that a new Act would be beneficial, and could incorporate amendments that we have recommended, such as the exemption of disclosures to legal advisers for the purpose of seeking legal advice. However, we recognise that there was little consensus amongst consultees about what ought to be included in any new legislation. For this reason, and given the strength of the concerns expressed by consultees, we consider that further in-depth consultation would need to take place should the decision ever be taken to repeal and replace the OSA 1989.

---

319 Dr Ashley Savage, p 8.

320 The Institute of Employment Rights, p 24.

Chapter 6: Miscellaneous unauthorised disclosure offences

INTRODUCTION

6.1 In our Consultation Paper, we surveyed and analysed 124 unauthorised disclosure offences.[321] Although at a high level of generality those offences share a common purpose, in that they criminalise unauthorised disclosure, we found considerable variety in drafting and a lack of a uniformity in approach.[322] We asked three questions seeking consultees' views on the need for a review, and on the scope of any such review.

6.2 This is in line with our terms of reference, agreed with the Cabinet Office in 2016, and noted at the beginning of this Report at paragraph 1.5.

DATA SHARING BETWEEN PUBLIC BODIES

6.3 The Law Commission has previously examined the law regulating data sharing by public bodies. We published a scoping report, "Data Sharing between Public Bodies", in July 2014 ("Scoping Report"). Our recommendations in this Chapter are intended to complement our recommendations in that Scoping Report.

6.4 In our Scoping Report, we concluded that the statutory framework for data sharing lacked a clear and principled approach.[323] We identified that one category of restriction on data sharing comprised criminal offences of unauthorised disclosure or misuse of information held for the performance of statutory functions.[324]

6.5 At the conclusion of the Scoping Report, we recommended that broader reform was needed to create a principled and clear legal structure for data sharing, which will meet the needs of society. These needs include efficient and effective government, the delivery of public services and the protection of privacy. We noted that data sharing law must also accord with what was then emerging European law and cope with technological advances. The reform should include work to map, modernise, simplify and clarify the statutory provisions that permit and control data sharing and review the common law.

6.6 We called for a comprehensive review of the law in Data Sharing Between Public Bodies. The government was simultaneously developing policy on how to reform

---

321 Consultation Paper, para 4.1.

322 CP, para 4.4.

323 Data Sharing between Public Bodies: A Scoping Report (2014), Law Com No 351, para 1.104.

324 Data Sharing between Public Bodies: A Scoping Report (2014) Law Com No 351, para 1.37.

certain areas of data sharing.[325] The ensuing Digital Economy Act 2017 contained reforms more limited than we had envisaged in our recommendation, however. It also increased the number of unauthorised disclosure offences and exacerbated the lack of a uniform, consistent and coherent approach in this area.

UNAUTHORISED DISCLOSURE OFFENCES AND THE PROTECTION OF OFFICIAL DATA

6.7 In our Protection of Official Data Consultation Paper, we argued that there was merit in considering reform of unauthorised disclosure offences irrespective of whether a broader reform project was undertaken examining statutory gateways for data sharing, as we had recommended in our project on Data Sharing Between Public Bodies.[326]

6.8 Many miscellaneous unauthorised disclosure offences criminalise the disclosure of "personal" information relating to identifiable individuals.[327] The offences often exist in connection with a legislative gateway for processing information by public bodies (which is a statutory power to share information, perhaps for a particular purpose, or with a particular public body).[328] In our Consultation Paper, we identified a lack of uniformity across the legislative landscape.[329] The offences we identified varied as to the conduct they criminalised,[330] the fault element required,[331] the extent to which onward disclosure by recipients was criminalised,[332] the defences and exemptions provided,[333] whether consent was required to prosecute,[334] and the maximum sentence provided.[335] Permitted disclosures were sometimes framed by statute as exemptions and sometimes as defences, with apparently arbitrary effects on which party would bear the burden of proof.[336]

6.9 We accepted that there might be good reason for the degree of inconsistency that we identified,[337] but the legislative landscape appeared to us to be irrational, dispersed and lacking in uniformity.[338] In our pre-consultation meetings with stakeholders,

---

325 Data Sharing between Public Bodies: A Scoping Report (2014) Law Com No 351, para 1.80.

326 CP, para 4.5.

327 CP, para 4.20.

328 CP, para 4.22.

329 CP, para 4.27.

330 CP, para 4.25.

331 CP, para 4.30.

332 CP, para 4.33.

333 CP, para 4.39.

334 CP, para 4.45.

335 CP, para 4.46.

336 CP paras 4.41 to 4.44.

337 CP, para 4.52.

338 CP, para 4.55.

however, there was no suggestion that this caused any pressing problems in practice.[339]

Consultation question 10

6.10 Consultation question 10 asked:

> Do consultees agree that a full review of personal information disclosure offences is needed?

6.11 As we discuss in detail below, the responses we received to our consultation have tended to confirm our initial impression. While consultees were generally supportive of a review, there was not much further evidence of practical problems being caused by the existence of various miscellaneous disclosure offences. A notable exception is the case of *Pytel v The Office for Gas and Electricity Market* ("OFGEM")[340] which is discussed below.

Consultation responses

6.12 Consultees generally welcomed the call for a full review.[341] We note in particular that the Information Commissioner recognised there was "scope for improvement" in this area.[342] In their joint response, the Bar Council and Criminal Bar Association considered that the Consultation Paper "amply makes out the case for a full review".[343] They pointed to a "lack of uniformity, coherence or strategy to the current plethora of offences such that the legal landscape is confusing and often unrealised" with "unjustified fear of the liabilities that might arise", a "consequent reluctance" to disclose even where permitted, and the "failure to hold individuals and organisations to account where material is improperly disclosed".[344]

6.13 The BBC agreed that there was a "strong case for a full review of disclosure offences"[345] and that the "confusing and inconsistent panoply of legislation may be contributing to what we believe is a general low level of understanding of rights and obligations regarding the disclosure of personal information".[346] The BBC suggested this had "resulted … in limited awareness of what actual restrictions there are and on occasion a reluctance or nervousness around sharing information even where this is permitted".[347]

6.14 Public Concern at Work considered that we had made a compelling argument that miscellaneous offences had proliferated "without consideration about whether some

---

339 CP, para 4.58.

340 Employment Tribunal Case No. 2206458/2016 (22 December 2016).

341 For example, Public Concern at Work, p 5; Campaign Against Censorship, p 1; Whistleblowers UK, p 3; A Savage, p 10; and the Crown Prosecution Service, p 7.

342 Information Commissioners Office, p 1.

343 Bar Council, page 12.

344 Bar Council, p 12.

345 BBC, p 5.

346 BBC, p 5.

347 BBC, p 5.

universal principles surrounding the question of public interest disclosures should apply to such offences".[348] It was considered that non-disclosure offences had been "drafted and passed with no thought given to how they impact [on] the public interest, or on whistleblowing more generally".[349] Public Concern at Work pointed out that non-disclosure offences can limit the availability of the Public Interest Disclosure Act 1998 to "whistleblowers".[350] This is because a disclosure is not a "protected disclosure" for the purposes of the Public Interest Disclosure Act 1998 if the person making the disclosure commits an offence by making it.[351] The proliferation of unauthorised disclosure offences therefore has the effect of eroding the protections available to employees under that legislation.

6.15 Public Concern at Work helpfully referred to *Pytel v OFGEM* to illustrate their point.[352] The case considered whether section 105 of the Utilities Act 2000 prevented the disclosure of relevant material in relation to a Public Interest Disclosure Act 1998 claim before the employment tribunal. In that case, it was common ground that section 105(1) covered the relevant material, and the disclosure for the purpose of proceedings under the Employment Rights Act 1996 was not on the list of disclosures to which section 105(1) did not apply.[353] As the effect of this would be to deprive the claimant of his rights under the Employment Rights Act 1996, the tribunal held that section 3 of the Human Rights Act 1998 and Articles 6 and 10 of the European Convention on Human Rights permitted the tribunal to read "Parts IVA and V of the Employment Rights Act 1996" into the list of disclosures to which section 105(1) does not apply.[354]

6.16 In response to consultation question 10, Peters and Peters observed that differences between individual offences may well be justified in some circumstances, and suggested that:

> whether a full review is required as a matter of priority should, ultimately be dependent upon an overall assessment of how well the current system has been working in practice.[355]

6.17 Trinity Mirror highlighted a concern that any review should only be conducted "in order to ensure that journalists can do their job properly in the public interest", including that "public interest defences should be available for all potential offences."[356]

---

348 Public Concern at Work, p 5.

349 Public Concern at Work, p 5.

350 Public Concern at Work, p 6.

351 Section 43B(3) Employment Rights Act 1996.

352 Public Concern at Work, p 6; *Pytel v OFGEM*, Employment Tribunal Case No. 2206458/2016 (22 December 2016).

353 Utilities Act 2000, s 5(4). *Pytel v OFGEM*, Employment Tribunal Case No. 2206458/2016 (22 December 2016) at [12].

354 *Pytel v OFGEM*, Employment Tribunal Case No. 2206458/2016 (22 December 2016) at [46].

355 Peters and Peters, p 11.

356 Trinity Mirror, by email.

6.18 Oliver Butler pointed out that unauthorised disclosure offences, even when limited to those protecting personal information or the identification of individuals, nevertheless shared an important connection to official secrecy offences. Moreover, Butler cautioned against reforming official secrecy without a wider review of unauthorised disclosure offences[357] because those offences "have more in common with official secrecy than the Consultation Paper suggests".[358] It was "inaccurate to characterise [personal information disclosure offences] as concerned with individual's rights and interests"[359] because "their function is to facilitate State projects by imposing penalties on unauthorised disclosures to engender greater trust in the public"[360] as the unauthorised disclosure "could damage public trust in the service being undertaken".[361]

6.19 Butler noted that both official secrecy and other unauthorised disclosure offences shared a common rationale in preventing damage to the effectiveness of certain state functions and reinforcing reliance on authorisation for disclosures or internal complaints mechanisms to resolve concerns.[362] Consistency was therefore desirable.[363] He added that it is relevant that "most [unauthorised disclosure offences] are modelled on the 1989 Act".[364] Butler observed that the "offences also sometimes share a legislative history with official secrecy that should not be neglected, as fragmentation and incoherence in the law were often the fruit of ad hoc legislative responses after 1989."[365] This was because the "proliferation of post-1989 offences is in large part a result of the narrowing of official secrecy in the 1989 Act".[366]

6.20 The News Media Association disagreed with the provisional proposal, submitting:

> The proposal for a further review of other unauthorised disclosure offences, under the same terms of reference and from the same perspective, could result in even greater criminalisation of journalism and restrictions on the public right to know.

Analysis

6.21 We agree with Dr Butler that, although many unauthorised disclosure offences are limited to the protection of information identifying individuals, their rationale is not exclusively the protection of personal information but also the interests of those public functions supported by effective data collection and processing.

6.22 Following our consultation and analysis of responses, we consider that the lack of uniformity in this area of law requires greater scrutiny. We remain concerned that the

---

357 O Butler, p 2.

358 O Butler, p 2.

359 O Butler, p 9.

360 O Butler, p 9.

361 O Butler, p 9.

362 O Butler, p 9.

363 O Butler, p 9.

364 O Butler, p 10.

365 O Butler, p 10.

366 O Butler, p 10.

ad hoc legislative history of unauthorised disclosure provisions has resulted in an inconsistent and confusing landscape which has the potential to inhibit proper disclosures and public interest journalism. The potential for the proliferation of unauthorised disclosure offences to have a chilling effect on lawful and desirable data sharing is a serious consideration to be taken into account in any future review. The fact that the offences concern restrictions on freedom of expression demands a coherent and clearly justified approach. The offences, although protecting individual information, have a rationale beyond data protection in enhancing the protection of data held by public bodies in order to help them perform their functions and secure public trust more effectively. This is a rationale and importance that goes beyond the concerns of section 55 of the Data Protection Act 1998 and its replacement in the Data Protection Act 2018 (see paragraph 6.28 and what follows). These are not concerned with particular features of the official context in which the processing occurs and which may be undermined by unauthorised disclosure.

6.23 We share the concern that the proliferation of unauthorised disclosure offences may have the effect of eroding the protections available to employees under the Public Interest Disclosure Act 1998. While the employment tribunal in *Pytel v OFGEM*[367] decided that the Utilities Act 2000 could be read to permit disclosure to by OFGEM to the tribunal, the matter was successfully appealed by OFGEM. In a judgment handed down at the Employment Appeal Tribunal on 10 December 2018, Mrs Justice Elisabeth Laing held that the Employment Tribunal had erred in its interpretation of section 105 of the Utilities Act 2000, and that it was not possible to read the provision so as to be compatible with Pytel's Article 6 and Article 10 rights under the ECHR. It followed from this decision that the Employment Tribunal's first instance "consequential directions about disclosure were wrong in law and are of no effect".[368]

6.24 Our understanding is that the decision is pending appeal. It is not therefore finally resolved whether it or similar offences will have the effect of preventing the disclosure necessary to advance claims under the Public Interest Disclosure Act 1998. We consider that this is an important consideration to take into account in reviewing the scope and operation of unauthorised disclosure offences.

6.25 We acknowledge Trinity Mirror's concern and consider that the potential for miscellaneous disclosure offences to restrict public interest journalism is a serious matter that should be taken into account in any review of miscellaneous unauthorised disclosure offences. This is especially true since government has recently recognised the importance of these protections in both the Data Protection Act 2018 and the Digital Economy Act 2017. Both contain express public interest defences. This recent development highlights the absence of such a defence in the many other disclosure offences.

6.26 Although a full review is not within the scope of the present project, we recommend a future review. We recognise that reform is not as pressing as in relation to our other recommendations, but nevertheless think a review of this area remains important. As we have already pointed out, the inclusion of a public interest defence in both the

---

367 *Pytel v OFGEM*, Employment Tribunal Case No. 2206458/2016 (22 December 2016).

368 *Pytel v OFGEM* [2018] UKEAT 0044_17_1012; [2019] ICR 715.

Digital Economy Act 2017 and the Data Protection Act 2018 makes the lack of such a defence in respect of the other offences seem especially problematic.

Recommendation 22.

6.27 There should be a review of unauthorised disclosure offences with the aim, in particular, of creating greater coherence and consistency in terms of the defences available and penalties that apply.

SECTION 55 OF THE DATA PROTECTION ACT 1998 / SECTION 170 OF THE DATA PROTECTION ACT 2018

6.28 In our Consultation Paper we asked whether section 55 of the Data Protection Act 1998[369] should be included in the scope of any future review. Section 55 made 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.[370] The provision has now been repealed and replaced by section 170 of the Data Protection Act 2018. Notably, section 170(1) reflects the elements of the previous section 55 offence and additionally criminalises the "unlawful retention of data".[371]

6.29 In our Consultation Paper, we identified two core problems with (the then) section 55 of the Data Protection Act 1998 (though these features persist in the new legislation). First, the maximum sentence was a fine.[372] We considered that this was especially problematic because advances in technology allow large quantities of personal information to be disclosed causing widespread harm.[373] The low maximum sentence was also undesirable as it resulted in prosecutions being brought on alternative charges, including misconduct in a public office and conspiracy to defraud, in order to make use of the higher maximum sentences attached to those offences.[374]

6.30 Secondly, we argued that section 55 mis-described the victim of the offence by focusing on the data controller who does not consent to processing rather than the data subjects affected by the unlawful processing.[375] In the Consultation Paper we commented that we found this "peculiar",[376] although we noted that the impact of the

369 Section 55 of the Data Protection Act 1998 has now been repealed and replaced by section 170 of the Data Protection Act 2018.

370 Data Protection Act 1998, s 55(3).

371 Explanatory Notes to the Data Protection Bill 2018.

372 CP, para 4.70.

373 CP, para 4.74.

374 CP, paras 4.75 and 4.76.

375 CP, para 4.79.

376 CP, para 4.81.

offence on the data subject is taken into account in sentencing.[377] We therefore suggested that a "more extensive review" of section 55 could be necessary.[378]

Consultation question 11

6.31 Consultation question 11 asked:

> 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 responses

6.32 The Information Commissioner welcomed our "examination and conclusions about the inadequacy of the current maximum sentence".[379] She argued that the "lack of a custodial sentence is more often than not neither adequate nor proportionate to the extent of criminality involved and does not provide a sufficient deterrent"[380] and that "criminals are exploiting the vacuum of a serious deterrent".[381] Controllers are not "supported by an effective deterrent".[382] The Information Commissioner observed that it was "common for the sentencing judge or magistrates to make comment at their surprise that their powers are limited to either a fine or discharge",[383] that "as financial penalties are linked to means, most penalties are low level",[384] and that "section 55 is not a recordable offence".[385]

6.33 Peters and Peters contended that the "maximum available sentence should be amended to imprisonment" and that "a maximum sentence of two years' imprisonment could appropriately reflect the harm done".[386] Oliver Butler argued that increasing the maximum sentence to two years' imprisonment would help to reduce reliance on other offences. He submitted that it might "go some way to release [the] pressure to pass unauthorised disclosure offences" because officials are often processors for a public authority data controller. He contended, however, that this approach had some limitations because sub-contractors might often be controllers in their own right and therefore not subject to the offence in section 55.[387]

6.34 Dr Ashley Savage was of the view that there was a "need for a review to determine [the] consistency of application" if unauthorised disclosures were both within the ambit

---

377 CP, para 4.82.

378 CP, para 4.84.

379 Information Commissioner's Office, p 3.

380 Information Commissioner's Office, p 3.

381 Information Commissioner's Office, p 3.

382 Information Commissioner's Office, p 3.

383 Information Commissioner's Office, p 4.

384 Information Commissioner's Office, p 4.

385 Information Commissioner's Office, p 4.

386 Peters and Peters, p 12.

387 O Butler, p 12.

of the 1989 and 1998 Acts.[388] The Bar Council, Criminal Bar Association and the Crown Prosecution Service were of the view that the section 55 offence should be encompassed within the full review.[389] Moreover, the BBC noted that "section 55… has been considered by parliament fairly recently" but considered "that this could usefully form part of a wider review…".[390]

6.35 Other consultees voiced concerns about a review of section 55. The News Media Association felt that the Consultation Paper's approach to sentencing and section 55 ignored "countervailing press freedom concerns".[391] Whistleblowers UK considered that section 55 offered "adequate protection and that a review is not necessary".[392] Global Witness argued that that there was no need to revisit custodial sentences for section 55 as this had been examined and rejected following an earlier consultation.[393] The Institute of Employment Rights argued that any review of section 55 should not examine section 55(2)(d), the public interest defence.[394] The Trinity Mirror contended that there should be "no custodial sentence" for section 55, and section 77 of the Criminal Justice and Immigration Act 2008 should be repealed, albeit that journalistic exemptions should be retained.[395]

6.36 The Information Commissioner disagreed with our suggestion that section 55 mis-describes the victim,[396] arguing that both data subjects and the controller can be victims of section 55,[397] in the case of a controller suffering "financial or reputational damage."[398] The Information Commissioner also highlighted that so describing the victim does not affect the data's subject's compensation rights.[399] In contrast, Peters and Peters submitted that "the victim of the offence is not clearly conceptualised" in the legislation, and contended that the offence "should be amended… to reflect the victim status of the data subject".[400]

6.37 Butler argued that the "Consultation Paper's treatment of section 55… fails to draw out some important differences between the offence and other statutory offences".[401] He argued that the section's "function differs from other unauthorised disclosure

---

388 A Savage, p 10.

389 The Bar Council and Criminal Bar Association, p 12; Crown Prosecution Service, p 8.

390 BBC, p 5.

391 New Media Association, p 1.

392 Whistleblowers UK, p 3.

393 Global Witness, by email.

394 Institute of Employment Rights, p 25.

395 Trinity Mirror, by email. Note that section 77 of the Criminal Justice and Immigration Act 2008 (which was never implemented) has now been repealed by schedule 19, paragraph 150 of the Data Protection Act 2018.

396 Information Commissioner's Office, p 2.

397 Information Commissioner's Office, p 2.

398 Information Commissioner's Office, p 2.

399 Information Commissioner's Office, p 2.

400 Peters and Peters, p 12.

401 O Butler, p 2.

offences"[402] and it "must be seen within the scheme of the Data Protection Act 1998"[403] where its "function is to enhance the control exercised by data controllers over the processing of personal data." To do this it "criminalises people other than the controller who process data contrary to the controller's authorisation"[404] and it is "therefore right that it is the data controller who is the 'victim' because it is the data controller's consent which is lacking".[405] He did not agree that the victim was mis-described.[406]

Analysis

6.38 We take the view that the offence in section 170 of the Data Protection Act 2018 is distinct from the miscellaneous unauthorised disclosure offences. It is based on a distinct rationale within the scheme of data protection law, namely to reinforce the control over processing exercised by the controller of personal data. Miscellaneous unauthorised disclosure offences on the other hand have a further rationale of supporting the proper performance of public functions. They do this by subjecting some officials and other recipients of data held by public bodies to criminal penalties in order to enhance public trust in data security.

6.39 Whilst we acknowledge the concerns of consultees relating to press freedom, we maintain the view that the maximum sentence in section 170 is too low adequately to address the most serious or damaging offending that falls within its scope. However, a review of miscellaneous unauthorised disclosure offences should consider where more narrowly defined offences could carry a higher maximum sentence than section 170 and therefore address our concerns without the need to apply a higher maximum sentence to the full range of wrongdoing covered by section 170.

6.40 The Data Protection Act 2018 did not increase the maximum sentence; it remains a fine.[407] We consider that this reinforces our conclusion that the offences in the data protection legislation are distinct from and much broader than the miscellaneous unauthorised disclosure offences we have identified. Although we remain concerned by the low maximum sentence attached to the offences in data protection legislation, we now consider that the better approach (as we recommend above) would be to review miscellaneous unauthorised disclosure offences and ensure that the most serious wrongdoing is adequately captured by those offences with effective penalties.

6.41 In relation to the concern expressed by those consultees representing the media, we note that the Data Protection Act 2018 includes a public interest defence that applies to the publication of journalistic material.[408]

---

402 O Butler, p 11.

403 O Butler, p 11.

404 O Butler, p 11.

405 O Butler, p 12.

406 O Butler, p 12.

407 See: Data Protection Act 2018, s 196(2).

408 Section 170(3)(c) of the Data Protection Act 2018.

6.42 Albeit that the offences in the Data Protection Act 2018 have only recently been enacted, if a comprehensive review were to be conducted then, for reasons of completeness and coherence, it would be sensible to include the Data Protection Act 2018.

Recommendation 23.

6.43 If a widescale review of the miscellaneous disclosure offences is conducted, it ought to include section 170 of the Data Protection Act 2018 for the sake of completeness and in an effort to ensure maximum coherence.

NATIONAL SECURITY DISCLOSURE OFFENCES

6.44 In our Consultation Paper, we defined "national security disclosure offences" as those offences that criminalise the unauthorised disclosure of information concerning national security, other than the Official Secrets Acts.[409] We examined seven offences[410] relating to national security, although we anticipated that there were likely to be some others.[411] We noted that the inconsistencies between national security disclosure offences were not as extensive as they were in relation to the personal information offences.[412] The two main inconsistencies we identified related to maximum sentences[413] and the requirement for damage.[414] We were unable to identify a principled reason to explain these inconsistent approaches.[415]

Consultation question 12

6.45 Consultation question 12 asked:

> Do consultees have a view on whether national security disclosure offences should form part of a future full review of miscellaneous unauthorised disclosure offences?

Consultation responses

6.46 Some consultees, such as the Crown Prosecution Service, were supportive of including national security disclosure offences within a wider review. Dr Ashley Savage argued that it was "vitally important that Crown servants are fully aware of the

409 CP, para 4.3.

410 These offences are: (a) the offence under section 11 of the Atomic Energy Act 1946; (b) the offence under section 13 of the Atomic Energy Act 1946; (c) the offence under section 79 of the Anti-terrorism, Crime and Security Act 2001; (d) the offence under regulations made in accordance with section 80 of the Anti-terrorism, Crime and Security Act 2001; (e) the offence under the Nuclear Industries Regulations 2003/403; (f) the offence under section 1 of the Armed Forces Act 2006; (g) the offence under section 17 of the Armed Forces Act 2006.

411 CP, para 4.86 onwards.

412 CP, para 4.104.

413 CP, para 4.105.

414 CP, para 4.106.

415 CP, para 4.109.

potential of breaching laws other than the Official Secrets Acts" and a review in light of Article 10 of the European Convention on Human Rights was necessary.[416]

6.47 However, the Bar Council and Criminal Bar Association suggested that the offences were "very different in nature to the personal information disclosure offences",[417] because the information was within the knowledge of fewer people, with training or special appointment, who understood its importance, so that "disclosure will entail a higher level of culpability".[418] Nevertheless, there was "scope for a consistency of approach"[419] and it was considered that these offences "merit attention within a wider review",[420] provided that there is "careful and proper attention to the special features of these offences that set them apart".[421]

6.48 Oliver Butler considered that national security offences are distinct from other unauthorised disclosure offences, noting that "where they relate to the nuclear and uranium industries, these do not necessarily involve official information"[422] and observing that certain "other offences relate to service law".[423] As a result, Butler considered that national security disclosure offences "could be excluded from the scope of the project".[424]

Analysis

6.49 We conclude that national security disclosure offences should be included within the scope of a review of miscellaneous disclosure offences. We acknowledge that they are likely to require a different approach to other unauthorised disclosure offences and it is important to pay close attention to context. They are relatively few in number, however, and relate to an important interest of the state. The fact that information relevant to this interest is sometimes produced by industries rather than officials is an important consideration in relation to the wider question of how far such offences should span across the public-private divide and apply to individuals who are neither officials nor government contractors. As we noted in our Scoping Report on Data Sharing Between Public Bodies, it is not always appropriate to draw a distinction between public and private bodies because public functions can be performed by a wide range of different organisations, both public and private.[425] It is furthermore desirable that any future review be comprehensive. We therefore recommend that national security disclosure offences be included within the scope of any future review.

---

416 A Savage, p 10.

417 Bar Council/Criminal Bar Association, p 12.

418 Bar Council/Criminal Bar Association, p 12.

419 Bar Council/Criminal Bar Association, p 12.

420 Bar Council/Criminal Bar Association, p 12.

421 Bar Council/Criminal Bar Association, p 12.

422 O Butler, p 10.

423 O Butler, p 11.

424 O Butler, p 2.

425 Data Sharing between Public Bodies: A Scoping Report (2014) Law Com No 351, para 1.96.

Recommendation 24.

6.50 National security disclosure offences should form part of the review of miscellaneous disclosure offences recommended above.

Chapter 7: Procedural matters relating to investigation and trial

INTRODUCTION

7.1 In Chapter 5 of our Consultation Paper, we examined a number of procedural matters relating specifically to prosecutions for offences contrary to the Official Secrets Acts – both 1911 and 1989 – that we believed were worthy of detailed consideration.

THE PROTOCOL

7.2 One of these matters was the "Protocol on Leak Investigations" ("the Protocol"), which sets out a standard procedure that ought to be followed before any police investigation for a suspected offence contrary to the Official Secrets Act 1989 is requested.

7.3 Unauthorised disclosures can be categorised in four ways. The Protocol is only concerned with the first two categories:

(1) unauthorised disclosures that are suspected to constitute Official Secrets Act 1989 offences engage the Protocol and should be referred to the Cabinet Office;

(2) unauthorised disclosures that are themselves, or are related to, other suspected "serious criminal offences"[426] engage the Protocol and should be referred to the Cabinet Office;

(3) unauthorised disclosures that are suspected criminal offences but do not engage the Official Secrets Act 1989 or otherwise concern the safety or interests of the state do not engage the Protocol.[427] They should be reported to the police by the organisation that has lost the information.

(4) unauthorised disclosures which are not criminal offences do not engage the Protocol. They are internal disciplinary/information security matters for the organisation that has lost the information. They should not be reported to the police.

---

[426] As defined below at 7.11.

[427] For example, an unauthorised disclosure of information contrary to section 105 of the Utilities Act 2000 is unlikely to concern the safety or interests of the State.

Background to the Protocol

7.4 The Protocol was first proposed by Her Majesty's Chief Inspectorate of Constabulary ("HMIC") in October 2009,[428] and adopted by the Government in March 2010.[429] The HMIC report was published as a result of an investigation into a series of leaks emanating from the Home Office. During the course of this investigation, both a civil servant and a Member of Parliament were arrested. In April 2009, the Director of Public Prosecutions announced that no charges would be brought against either individual.[430]

7.5 As a result of the unusual and high-profile nature of this case, a series of reviews were undertaken. In particular, the Home Secretary asked HMIC 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".[431] As we set out in the Consultation Paper, the HMIC report concluded that the police should not investigate leaks which only have the effect of causing embarrassment to the Government or cause no more disruption to the effective running of Government Departments than any leak would inevitably carry.[432] HMIC recommended the adoption 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 Protocol describes a process which encourages key stakeholders to contribute to the decision making, whilst recognising the independence of each organisation. The aim is to apply a discipline of supportive, collective reasoning to a wide range of considerations including likelihood of success and assessment of outcomes.[433]

---

428 Her Majesty's Inspectorate of Constabulary, Review of the Lessons Learned from the Metropolitan Police Service's Investigation of Home Office Leaks (October 2009), available at https://www.justiceinspectorates.gov.uk/hmicfrs/media/lessons-learned-report-20091001.pdf.

429 See Her Majesty's Inspectorate of Constabulary, Review of the Lessons Learned from the Metropolitan Police Service's Investigation of Home Office Leaks (October 2009) Annex B, available at https://www.justiceinspectorates.gov.uk/hmicfrs/media/lessons-learned-report-20091001.pdf; and Government Response to the Tenth Report of Session 2008-09 from the Public Administration Select Committee: Leaks and Whistleblowing in Whitehall (March 2010) Cm 7863 Annex A, available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/228774/7863.pdf.

430 See, eg R Edwards and T Whitehead, *Damian Green arrest: no charges over Home Office leaks* (16 April 2009), available at https://www.telegraph.co.uk/news/politics/5163574/Damian-Green-arrest-no-charges-over-Home-Office-leaks.html.

431 Her Majesty's Inspectorate of Constabulary, Review of the Lessons Learned from the Metropolitan Police Service's Investigation of Home Office Leaks (October 2009) para 4.7, available at https://www.justiceinspectorates.gov.uk/hmicfrs/media/lessons-learned-report-20091001.pdf.

432 Her Majesty's Inspectorate of Constabulary, Review of the Lessons Learned from the Metropolitan Police Service's Investigation of Home Office Leaks (October 2009) Annex B, available at https://www.justiceinspectorates.gov.uk/hmicfrs/media/lessons-learned-report-20091001.pdf.

433 Her Majesty's Inspectorate of Constabulary, Review of the Lessons Learned from the Metropolitan Police Service's Investigation of Home Office Leaks (October 2009) para 9.4, available at https://www.justiceinspectorates.gov.uk/hmicfrs/media/lessons-learned-report-20091001.pdf.

7.6 The Protocol was annexed to the report.[434] It set out a seven-step process for investigating leaks. The report stated that in future leak investigations there should be a presumption in favour of the police not being involved unless there are:

(1) reasonable grounds for believing an offence under the Official Secrets Act 1989 has been committed; or

(2) reasonable grounds for believing a "serious criminal offence" has been committed as an integral part of a leak(s), such as the example where an official is subject to bribery or corruption, or very exceptional cases which seriously threaten the UK in economic or integrity terms.

The seven-step process

7.7 Below we reproduce the seven-step process recommended by HMIC and subsequently adopted by the government:

> 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 Metropolitan Police Service the level has been suggested at Deputy Commissioner. The Director of Public Prosecutions and Commissioner of the Metropolitan Police

---

[434] See Her Majesty's Inspectorate of Constabulary, Review of the Lessons Learned from the Metropolitan Police Service's Investigation of Home Office Leaks (October 2009) Annex B, available at https://www.justiceinspectorates.gov.uk/hmicfrs/media/lessons-learned-report-20091001.pdf.

Service 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 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 (“CPS”) 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, CPS 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

> 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.

7.8 In our Consultation Paper we concluded that the Protocol fulfils an important function. However, we also thought that improvements could be made.

Provisional conclusion 18

7.9 Provisional conclusion 18 stated:

> We provisionally conclude that improvements could be made to the Protocol. Do consultees agree?

7.10 We asked consultees for their views on whether it is necessary to clarify the types of criminal offence to which the Protocol 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 other compelling grounds to believe that some other "serious offence" has been committed as an integral part of the leak. The term "serious offence" is defined in the introduction to the draft Protocol:

> for example where an official is subject to bribery or corruption, or very exceptional cases which seriously threaten the UK in economic or integrity terms.[435]

7.11 We considered that there was the possibility that this definition could be misconstrued and suggested that arguably, it should only be those serious criminal offences *where the conduct has implications for national security* that should engage the Protocol. We also asked consultees for their views on whether it was desirable to ensure that there is earlier legal involvement in the process from, for example, the CPS. 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 could be identified at an early stage.

Consultation questions 13 and 14

7.12 Consultation question 13 asked:

> Do consultees have a view on whether defining the term "serious offence" and ensuring earlier legal involvement would make the Protocol more effective?

7.13 Finally, consultation question 14 asked:

> Do consultees have views on how the Protocol could be improved?

---

[435] Her Majesty's Inspectorate of Constabulary, Review of the Lessons Learned from the Metropolitan Police Service's Investigation of Home Office Leaks (October 2009) Annex B, available at https://www.justiceinspectorates.gov.uk/hmicfrs/media/lessons-learned-report-20091001.pdf.

Consultation responses

7.14 Few consultees engaged with these consultation questions and we are grateful to those who did.[436]

7.15 The Campaign Against Censorship stated that the Protocol ought to be incorporated into legislation to ensure that members of the public are made aware of its existence.[437] The CPS agreed that improvements could be made to the Protocol. It agreed that defining "serious offence" and ensuring earlier legal involvement would be steps worth taking.[438]

Versatility

7.16 In their joint response, the Bar Council and the Criminal Bar Association agreed that the Protocol could be improved. They expressed the concern that the Protocol may be insufficiently versatile where the investigation is not concerned with leaks of politically embarrassing material, but with disclosures that are intended to compromise national security. They stated:

> Any "gateway process" must not lose sight of this far more serious dimension and must allow for a swift and robust response where appropriate.[439]

7.17 The Bar Council and Criminal Bar Association suggested that the Protocol should be more easily adaptable and should reflect the range of situations to which it could be applied:

> One of the stated aims of the Protocol was its versatility and to ensure the necessary sensitivity where a high profile public figure (such as a Member of Parliament) is the subject of an investigation. One concern is that the Protocol may not be sufficiently versatile where the investigation is not concerned so much with strategic political "leaks" as with criminal disclosure intended to compromise national security.[440]

Serious offence

7.18 The Bar Council and Criminal Bar Association disagreed with our provisional view that the term "serious offence" ought to be defined as it would be difficult to predict when the Protocol should be invoked. They stated that:

> Examples include the incremental damage caused by a series of unauthorised disclosures (where the specific instances of unauthorised disclosure would not themselves seem so serious); the persons involved in the unauthorised disclosures, particularly where an individual has access to information by reason of special training, appointment or circumstances; the persons to whom the information is

---

436 In particular, we thank the Bar Council and Criminal Bar Association, the Campaign Against Censorship, the Crown Prosecution Service, the Institute of Employment Rights, Peters and Peters Solicitors LLP, and Dr Ashley Savage.

437 Campaign Against Censorship.

438 Crown Prosecution Service, para 27.

439 Bar Council / Criminal Bar Association, para 62.

440 Bar Council / Criminal Bar Association, para 62.

disclosed; the means by which the information is disclosed; or where the individual concerned is the holder of elected office. Rather than defining "serious offence", a sensible course would be to outline factors that should be taken into account by the decision maker when determining whether an offence is sufficiently serious. This would allow decisions to be made on a case by case basis.[441]

7.19 Peters and Peters considered that the term "serious offence" should be defined to ensure both consistent interpretation of this term and consistent application of the criteria set out in the Protocol for determining whether the threshold for police involvement has been reached:

> We note that the Protocol is used throughout all Government departments when dealing with unauthorised disclosures, and, lacking any detailed guidance as to what constitutes a serious offence, the interpretation of the term could vary significantly depending on experience, training or personal perception.[442]

7.20 In terms of how "serious offence" ought to be defined, Peters and Peters suggested that an exhaustive list of offences that constitute a "serious offence" could be formulated. Further, they suggested that it should be capable of amendment, similar to the list of offences that are never filtered for the purpose of criminal records checks by the Disclosure and Barring Services. It was suggested that such a list would eliminate unnecessary uncertainty.[443]

7.21 In his response, Dr Ashley Savage agreed that the term "serious offence" ought to be defined and suggested that a non-exhaustive list would be useful in this regard.[444] A member of the public who responded to our consultation, Jim Pragnell, also agreed that the term "serious offence" should be defined, arguing that "without definitions the government and our intelligence services can decide for themselves what these terms mean".[445]

Law enforcement engagement

7.22 Dr Savage also called for clarification as to what additional guidance may be relied upon to determine the circumstances where police involvement would be considered appropriate. He stressed that it was important that any guidance used in determining the outcomes of the various steps of the protocol is sufficiently clear and is legally accurate. In particular, Dr Savage considered that stages two, three and five of the Protocol needed clarification:

> Step two, for example, states that "consideration should be given to the proportionality of police involvement…" It would be useful to clarify what additional

441 Bar Council / Criminal Bar Association, para 63.

442 Peters and Peters, p 13.

443 Peters and Peters, p 13.

444 A Savage, para 33.

445 Jim Pragnell, by email.

guidance is provided beyond the protocol to determine the circumstances where involvement would be considered appropriate.[446]

7.23 Dr Savage drew our attention to the guidance produced by the CPS entitled "Prosecuting Cases Where Public Servants Have Disclosed Confidential Information to Journalists",[447] which covers some of the same ground as the protocol. He noted in passing that it was potentially misleading as it did not refer to recent case law of the European Court of Human Rights.[448]

7.24 Peters and Peters agreed that early legal involvement would be desirable. They pointed out that the involvement of the CPS is only mentioned at Stage 5 of the Protocol, by which point a determination would presumably already have been made of whether a "serious offence" may have been committed. They suggested that it would be an improvement to make clear that when a police investigation has commenced the independence of that investigation must be maintained at all times.[449]

7.25 The Institute of Employment Rights stated:

> Any redrafting of the Protocol should ensure the involvement of the police in the investigation of unauthorised disclosures is only in exceptional circumstances and also the independence of the police from the Executive is maintained.[450]

7.26 The Government Response agreed that the Protocol should be reviewed.

Analysis

7.27 Consultees all agreed that the Protocol could be improved. This is unsurprising given that the Protocol is ten years old, and a response to particular circumstances.

7.28 We agree with the Campaign Against Censorship that there ought to be greater awareness that the Protocol exists. We do not, however, believe that enshrining it in legislation is the best way of achieving this aim. We cannot assume that putting things in statute ensures that they are well known. There are thousands of statutory offences, but very few people are aware of more than a few of them. Placing the Protocol on a statutory footing would also make it difficult to amend, thus losing the flexibility that other stakeholders considered to be important. We consider that the recommendations we make below (a review of the Protocol, with consultation, and that it should thereafter be made available online) would have the additional benefit of raising awareness about it.

7.29 With regard to defining the term "serious offence", consultees generally agreed that the current wording was vague, but they did not agree on how best to improve it. It is worth reiterating that the term serious offence is being used in a very specific manner

---

446 A Savage, para 34.

447 See Crown Prosecution Service, *Media: Prosecuting Cases Where Public Servants Have Disclosed Confidential Information to* Journalists (27 July 2009), available at https://www.cps.gov.uk/legal-guidance/media-prosecuting-cases-where-public-servants-have-disclosed-confidential.

448 A Savage, para 35.

449 Peters and Peters, p 14.

450 Institute of Employment Rights, p 26.

in this context. It is not being used to describe a general category of offences that might typically be regarded as serious, such as murder. It is used to denote that certain offences involving unauthorised disclosure will be so serious that they deserve to be dealt with under the Protocol. In other words, it is not enough to ask whether the offence is one of a type relating to unauthorised disclosures that we might want to label as serious; we would also want to ask whether the gravity of the wrong or its consequences in the particular case was sufficient to render it "serious" even if it was within the category of disclosure offences that we might naturally label as serious. It is unlikely, then, that a simple list of "serious" offences would be sufficient for the purpose of engaging the Protocol.

7.30 We consider that a balance needs to be struck between allowing sufficient flexibility to respond to unexpected circumstances, whilst also guarding against the Protocol being used inappropriately for trivial offences. A non-exhaustive list of offences is one approach. However, as the Bar Council / Criminal Bar Association noted, a relatively low level, unauthorised disclosure might not be significantly serious on its own, but depending on the person or Department from which it emanated, and if there was evidence of a pattern of behaviour, it might become so. Alternatively, or in addition to a non-exhaustive list, the types of situation in which the Protocol should be followed could be defined.

7.31 We agree with Peters and Peters that a lack of clear definition of what amounts to a "serious offence" risks the Protocol being applied inconsistently. One way in which this risk is mitigated in practice is through internal departmental procedures across Whitehall. References to the Protocol are only made once a Department has followed its own security process. In practice, that means that references to the Protocol come via the lead officials on security within Departments.

7.32 We see some merit in Peters and Peters' suggestion that an exhaustive list of offences that constitute "serious offences" should be compiled, because undoubtedly this would promote certainty, though equally this may risk being insufficiently flexible.

7.33 We see the sense of the Bar Council and Criminal Bar Association's suggestion that it could be helpful to outline factors that should be taken into account by the decision-maker when determining whether an offence is sufficiently serious in this context. It might also be possible for the Government to make clear which unauthorised disclosure offences will not normally be considered a "serious offence" for the purposes of the Protocol, though we recognise that these offences are numerous, so this will be a difficult exercise. Nonetheless, we make no recommendation on how "serious offence" should be further defined. This would be better settled during the proposed review of the Protocol.

7.34 Dr Ashley Savage pointed out that the CPS guidance on prosecuting cases where public servants have disclosed confidential information to journalists had not been updated to reflect Article 10 case law developments. Despite recently being updated in November 2019, we saw scope for further and more particular reference to developments in ECHR case law.

7.35 The CPS guidance on prosecuting cases where public servants have disclosed confidential information to journalists was not reviewed in our Consultation Paper. The CPS guidance will not apply to all cases that come through the Protocol, but there are

clearly some cases where it will. The CPS should be aware that some types of case go through the Protocol. Similarly, the police and other users of the Protocol should be aware of the guidance the CPS will apply when deciding whether to prosecute public servants who have disclosed confidential information to journalists. We therefore think that the CPS guidance should make reference to the Protocol and vice versa. This will ensure maximum clarity and consistency across the decision-making process.

7.36 We agree with consultees who called for greater accessibility of the Protocol. Whilst it is available online, it is only accessible via the appendix to the HMIC report from 2009 and in the Government's response to the Public Administration Select Committee's Report on Leaks and Whistleblowing in Whitehall.[451] It would not require much resource to place the protocol somewhere more obvious, such as the Cabinet Office section of the GOV.UK website.[452]

7.37 We note the point made by the Institute of Employment Rights about restricting police involvement in such cases to exceptional circumstances. The majority of leaks do not constitute suspected offences under the Official Secrets Act 1989 or other "serious offences" as defined in the Protocol and will therefore not engage the Protocol. However, where there are reasonable grounds to suspect a criminal offence has taken place, it is quite proper for the police to be involved. Furthermore, we consider that the Protocol respects the independence of the police. For example, step three highlights the independence of the police and makes clear that at any stage the police may act outside of the Protocol and start or finish an investigation of their own accord, providing the situation is exceptional and there is a transparent rationale for taking such action.

7.38 We consider that the Protocol could benefit from external oversight in its operation. We appreciate that this is a sensitive matter, but consider that a requirement to report, perhaps to Parliament annually or biennially, would increase confidence in the Protocol and ensure it continues to evolve to meet the needs of interested parties.

Recommendation 25.

7.39 The Protocol on Leak Investigations should be reviewed and updated, in consultation with Government Departments, the Crown Prosecution Service, the Metropolitan Police, the Attorney General, and any other interested parties.

---

451 Government Response to the Tenth Report of Session 2008-09 from the Public Administration Select Committee: Leaks and Whistleblowing in Whitehall (March 2010) Cm 7863 Annex A, available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/228774/7863.pdf.

452 See, eg GOV.UK, *Cabinet Office*, available at https://www.gov.uk/government/organisations/cabinet-office.

Recommendation 26.

7.40 Consideration should be given, as part of the review of the Protocol, to an appropriate mechanism for providing oversight of its operation.

Recommendation 27.

7.41 The Crown Prosecution Service guidance "Prosecuting Cases Where Public Servants Have Disclosed Confidential Information to Journalists" should be updated to reflect developments in case law and to make reference to the Protocol.

Recommendation 28.

7.42 The Protocol should be published more accessibly online with information stating when it came into force, and detailing any revisions.

THE ABILITY TO EXCLUDE MEMBERS OF THE PUBLIC FROM THE COURT DURING PROCEEDINGS

7.43 In our Consultation Paper, we examined the fundamental principle of open justice. In *Scott v Scott*, Lord Shaw of Dunfermline described publicity in the administration of justice as "one of the surest guarantees of our liberties".[453] The courts have recognised, however, that open justice is not an absolute principle, and can be subject to exceptions. In *Attorney General v Leveller Magazine Ltd*, Lord Diplock stated that:

> … 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.[454]

---

453 *Scott v Scott* [1913] AC 417, p 476.

454 *Attorney General v Leveller Magazine Ltd* [1979] AC 440, p 450.

7.44 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".[455]

7.45 As we discussed in our Consultation Paper, 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 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.

7.46 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". By virtue of section 11(4) of the Official Secrets Act 1989, this also applies to the OSA 1989 offences. This statutory power exists 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.[456]

7.47 In our Consultation Paper, we found it 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 set out in *Scott v Scott* and affirmed in more recent cases.[457] 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

---

455 *Scott v Scott* [1913] AC 417, p 438.

456 *Attorney General v Leveller Magazine* [1979] AC 440, p 470. See also ML Friedland, *National Security: The Legal Dimension* (1979) p 46.

457 See, eg *Guardian News and Media Ltd v R & Erol Incedal* [2016] EWCA Crim 11; [2016] 1 WLR 1767.

care the argument in favour of secrecy, but it will often happen that something less than formal proof is all that is available.[458]

7.48 Although the point was not addressed directly when that 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 hearing evidence in a criminal case in camera was necessary in the interests of the due administration of justice.[459]

7.49 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. In our Consultation Paper we provisionally concluded that the exercise of this power should be made subject to the stricter test of necessity and that ideally this should be made explicit within a reformed statute.

Provisional conclusion 19

7.50 Provisional conclusion 19 stated:

> 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?

Consultation responses

7.51 The response to this provisional conclusion was generally favourable. Those consultees representing the media who responded to this issue, largely welcomed the proposal. For example, News Group Newspapers agreed with provisional conclusion 19, as did Dr Ashley Savage, the Campaign Against Censorship and Whistleblowers UK. Peters and Peters also agreed, stating:

> In our view, this amendment is required so that the limitations on the power conferred on the court by section 8(4) are aligned with the remit of the court's common law power to hear matters in private. Moreover, we note that the necessity test, due to its more precise wording and the existing common law guidance on its interpretation, would offer both (i) a more stringent legal test; and (ii) a more certain outcome than the current statutory wording of "prejudicial", thus ensuring that the fundamental principle of open justice is maintained where possible.[460]

---

458 *Attorney General v Leveller Magazine* [1979] QB 31, pp 44 to 45.

459 *Attorney General v Leveller Magazine* [1979] AC 440, p 451.

460 Peters and Peters, p 14.

7.52 The BBC agreed, but added a note of caution:

> The BBC … welcomes the Law Commission's recognition that the power conferred by section 8(4) to exclude the public must only be exercised [in] cases of necessity. Further, we agree that the necessity in question must be to ensure public safety. We believe that the precise phrasing here is important since the requirement of necessity would be diluted if what was being guarded against was any prejudice to national safety since national safety can be prejudiced whilst still being ensured. For example, the publication of information might result in resources needing to be redeployed or additional measures being taken. Having to take such steps might be prejudicial to national security but, provided national security could still thereby be ensured, the public interest in open justice would, we submit, dictate that the evidence be given in public.[461]

7.53 Professor Lorna Woods, Dr Lawrence McNamara and Dr Judith Townend agreed with provisional conclusion 19, but were "cautious, limited and conditional" in their agreement. They submitted that a test of necessity would be an improvement upon the current law, but would ultimately be insufficient to ensure respect for the rule of law. They emphasised that "neither the common law after *Incedal*[462] nor the Official Secrets Act provisions (as they are or as modified by the Commission's proposals) provide adequate protections for open justice".[463]

7.54 Specifically, they argued that the judgment in *Incedal*[464] exhibits a number of defects that merit review. For example, they queried whether it was sufficient for the court to permit "a limited number of 'accredited journalists'" to attend otherwise closed hearings:

> … the media may not always be the best or most effective representatives of the public interest. We should be cautious about both the process and the media's role. It is not at all inconceivable that journalists will moderate the way they report so that they do not risk their "accreditation".[465]

7.55 The BBC also expressed concerns regarding the *Incedal* judgment. It contended that the fact "a small number of accredited journalists" were permitted to attend the trial, but not to retain their notebooks nor publish any information arising from the trial was an "empty nod to the open justice principle."[466]

---

461 BBC, pp 6 to 7.

462 *Guardian News and Media Ltd v R & Erol Incedal* [2016] EWCA Crim 11; [2016] 1 WLR 1767. This was an appeal (ultimately dismissed) by the Guardian and others against reporting restrictions concerning parts of a terrorism trial that had been held in private. The Court of Appeal confirmed that, in exceptional circumstances, courts could depart from the principle of open justice. The test is narrow and strict: without excluding the public, justice cannot be done. The Court of Appeal found that the evidence in this case supported holding part of the trial in private in the interests of justice.

463 L Woods, L McNamara and J Townend, para 4.14.

464 *Guardian News and Media Ltd v R & Erol Incedal* [2016] EWCA Crim 11; [2016] 1 WLR 1767.

465 L Woods, L McNamara and J Townend, para 4.12.

466 BBC, p 7.

7.56 Guardian News and Media disagreed with provisional conclusion, arguing that the test was incorrectly formulated as one of necessity "to ensure national safety", whereas the power should be exercisable only if "necessary in the interests of the due administration of justice".[467] Guardian News and Media emphasised that "open justice is fundamental, and processes should not be permitted, deployed or encouraged which favour secrecy over transparency". It stated that:

> overall, while a necessity test [as defined in the Consultation Paper] is preferable to the existing test, the retention of the overall position of s 8(4) is not supported.[468]

7.57 The CPS also disagreed with the provisional conclusion, but on the grounds that it:

> … is a high bar to reach and would make it less likely that we would satisfy it, leading to a potential reduction in prosecutions.

7.58 The Bar Council and Criminal Bar Association also disagreed with the provisional conclusion. They questioned whether a statutory test is necessary in light of the existing common law, which they argued retains the flexibility that is possibly missing from the proposed test.[469]

7.59 In addition, the Bar Council and Criminal Bar Association argued that the proposed statutory test "seems more stringent" than the common law test, which "could confuse the legal landscape". They also argued that it would be difficult to apply in a number of circumstances, including where any prejudice to national safety is incremental and indirect, and where "the prejudice would be faced by a group outside of the nation" such as any information compromising the security or economic integrity of an ally.[470]

Analysis

7.60 With various qualifications, primarily based on the importance of promoting open justice, consultees have largely agreed that the inclusion of a necessity test in section 8(4) of the Official Secrets Act 1920 will improve the current provision.

7.61 We acknowledge the concerns expressed by the CPS that the inclusion of a necessity test will create a higher bar to reach and lead to a possible reduction in prosecutions. However, we consider it important that the limitations on the power conferred on the court by section 8(4) of the Official Secrets Act 1920 should be consistent with the common law position regarding the power of courts to hear trials in private.

7.62 At present, the wording of section 8(4) suggests that the public can be excluded from a trial or a part of a trial following a prosecution submission that their presence would be "prejudicial to the national safety". This gives the impression of a less rigorous test than at common law.

---

467 The Guardian, p 74.

468 The Guardian, p 75. The response deals with the issues in far greater detail and is available in full on our website.

469 The Bar Council and Criminal Bar Association, para 65.

470 The Bar Council and Criminal Bar Association, para 65.

7.63 We agree with Peters and Peters that the necessity test, with existing common law guidance on its interpretation, would provide a more stringent legal test and a more appropriate approach when considering any limitations on open justice. Indeed, it is clear from common law that the administration of justice should be the primary focus. Therefore, the test should be formulated accordingly. The power conferred on the court under section 8(4) ought to be subject to a necessity test, such that the exclusion of members of the public must be necessary for the administration of justice having regard to the risk to national safety.

7.64 In light of the existing lack of clarity, and for the avoidance of any doubt, we think it important that it be made clear on the face of the statute that the power to exclude the public in section 8(4) of the Official Secrets Act 1920 should only be exercised in cases of necessity.

Recommendation 29.

7.65 We recommend that the power conferred on the court by section 8(4) of the Official Secrets Act 1920 ought to be subject to a necessity test, such that the exclusion of members of the public must be necessary for the administration of justice having regard to the risk to national safety (replacing the term used in the 1920 Act: "prejudicial").

JURY CHECKS

7.66 In our Consultation Paper, we observed that section 118 of the Criminal Justice Act 1988 abolished the right of the defence to challenge jurors without cause.[471] 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.

7.67 Use of the right of "stand by", as it is known, is strictly speaking limited to those cases which involve national security or terrorism.[472] 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.[473]

7.68 The guidelines make clear that the authority to use this power must be personally given by the Attorney General, on the application of the Director of Public Prosecutions. The guidelines we included in our Consultation Paper remain the most recent version, and they are reproduced again here:[474]

---

471 J Gobert, "The peremptory challenge - an obituary" [1989] *Criminal Law Review* 528.

472 Governed by Criminal Procedure Rules (2015), rule 25.8(3). Discussed in D Ormerod and D Perry (eds), *Blackstone's Criminal Practice* (2020), at D13.22 to D13.45, and Appendix 2.

473 For early analysis, see A Nicol, "Official Secrets and Jury Vetting" [1978] *Criminal Law Review* 284.

474 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* (2019), at D13.45 and Appendix 2.

(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.

(a) There are, however, certain exceptional types of cases 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 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.

(3) 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.

(4) 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.

(5) 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.

(6) 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.

(7) 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.

(8) 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.

(9) Information revealed in the course of an authorised check must be considered in line with the normal rules on disclosure.

(10) 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.

(11) 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.

7.69 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.[475]

7.70 Given that some of the offences in 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. In view of the nature of cases involving terrorism and cases that touch upon national security, we took the provisional view in our Consultation Paper that this process continues to fulfil an important role in the context of the Official Secrets Acts. Moreover, our initial consultation with stakeholders, prior to publication of the Consultation Paper, did not indicate 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.

7.71 However, in our Consultation Paper, we did suggest that the guidance ought to be amended by making clear that, if authorised jury checks have been undertaken, this is brought to the attention of the legal representatives for the defence. We observed that 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

7.72 Provisional conclusion 20 stated:

> 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?

Consultation responses

7.73 The CPS did not express a view on provisional conclusion 20, and suggested it was a matter for the Attorney General.

7.74 The Institute of Employment Rights agreed with the provision conclusion and added:

> The vetting of members of the jury should be exceptional and if undertaken this infringement of the random selection principle is so significant, transparency is "vital" and so the defence must be informed.[476]

7.75 The Bar Council and Criminal Bar Association recommended caution:

> Particular care is required in this area … the absence of a right to challenge the decision to conduct a jury check, or the extent of the check, raises questions as to what benefit there can be in routinely sharing such information. The proposed reform would have to be carefully justified together with guidance on the use that could be made of any disclosed information.[477]

---

475 Crown Prosecution Service, *Jury Vetting* (10 July 2018), available at https://www.cps.gov.uk/legal-guidance/jury-vetting.

476 The Institute of Employment Rights, p 27.

477 Bar Council and Criminal Bar Association, para 66.

Analysis

7.76 We have reviewed the position on jury checks as part of our analysis of open justice matters relating to the project.

7.77 These procedures can serve a useful purpose because jurors who sit on OSA trials will be trusted with very sensitive information which could damage national security in the wrong hands. That is not to suggest that jurors would deliberately breach the confidentiality imposed on them in the trial process, or at least not many would do so. Serving on a jury hearing such evidence which is withheld from the public in the *in camera* sessions of the trial would be an unwelcome burden for some and would potentially expose jurors to being the target for hostile state agents who might seek to discover what sensitive information was disclosed. Jurors would have a lifelong obligation to retain confidentiality.

7.78 It is vital, however, that the jury system retains the complete confidence of the defence, and the public at large. To respect that, it is important that defence practitioners and the trial judge (as well as those prosecuting) are aware that jury vetting has occurred in the case.

Recommendation 30.

7.79 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 and the judge.

ISSUES THAT APPLY MORE GENERALLY TO CRIMINAL TRIALS IN WHICH SENSITIVE INFORMATION MAY BE DISCLOSED

7.80 While our Consultation Paper focused primarily on issues in the context of a trial involving the Official Secrets Acts, we were conscious that these issues could also arise in the context of any criminal trial that involves the disclosure of information that relates to national security. 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. 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. The Judicial College guide on Reporting Restrictions in the Criminal Courts noted that there are three stages in assessing the necessity for an order under section 4(2):

> The first question is whether reporting of the proceedings would give rise to a substantial risk of prejudice to the administration of justice. If not, that is the end of the matter.
>
> If there is a substantial risk of such prejudice, the court must ask whether a s.4(2) order would eliminate that risk. If not, there could be no necessity to impose a ban.

> Even if a judge is satisfied that the order would achieve the objective, he should still ask whether the risk can be overcome by less restrictive means. If so, a s.4(2) order could not be said to be necessary.
>
> If the judge is satisfied that the order is necessary, he has a discretion and must balance the competing public interests between protecting the administration of justice and ensuring open justice and the fullest possible reporting of criminal trials. An order under s.4(2) should be regarded as a last resort.[478]

7.81 This last position was echoed in *R v Sarker* by Lord Burnett of Maldon, now Chief Justice, who commented that "Reporting restrictions orders are therefore derogations from the general principle of open justice. They are exceptional, require clear justification and should be made only when they are strictly necessary to secure the proper administration of justice."[479]

7.82 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.

7.83 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. In this section we briefly describe these changes, without commenting on whether they manage successfully to reconcile the two imperatives outlined in the previous paragraph.[480] 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 process has received relatively little attention when compared with the civil process.

7.84 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 material being disclosed to non-governmental parties to the case.[481] 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 non-governmental parties to the case.

7.85 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

---

478 Judicial College, *Reporting Restrictions in the Criminal Courts* (May 2016) p28.

479 *R v Sarker* [2018] EWCA Crim 1341 at [29] (Lord Burnett of Maldon).

480 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.

481 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.

person and that it is in the interests of fair and effective administration of justice in the proceedings to make such a declaration. In proceedings such as these, a special advocate may be appointed to represent the interests of a party in closed material proceedings.[482]

7.86 These amendments to the law were enacted following recommendations in the Justice and Security Green Paper that was published in October 2011,[483] 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.

7.87 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.

7.88 In contrast to the civil law, the criminal law still relies upon the common law and on legislation not necessarily drafted with the aim of reconciling the competing interests. The fact there has been no systematic review perhaps explains why the common law test governs when it is legitimate to depart from the principle of open justice. That test 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.[484] 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. We have recommended (Recommendation 24) that the necessity test be formulated such that regard is had to the risk to national security subject to the primary focus being on the administration of justice.

Provisional conclusion 21

7.89 Provisional conclusion 21 stated:

> 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?

---

482 In the criminal context special counsel may be used. For discussion, see J Jackson, *Special Advocates in the Adversarial System* (1st ed 2019); and J Jackson, "The role of special advocates: advocacy, due process and the adversarial tradition" 20(4) (2016) International Journal of Evidence and Proof 343.

483 Justice and Security Green Paper (2011) Cm 8194.

484 The extent to which these two tests differ as a matter of substance is debatable.

Consultation responses

7.90 The Crown Prosecution Service agreed with the proposal, as did the Bar Council/Criminal Bar Association, Dr Ashley Savage, Campaign Against Censorship, the BBC and Peters and Peters.

7.91 The Bar Council/Criminal Bar Association stated:

> This is an area that is likely to be encountered in the courts with increasing frequency. Clear guidance as to how to deal with such situations is required.[485]

7.92 While agreeing that a separate review is warranted, the BBC stated:

> Closed Material Procedures represent a radical, but relatively new, departure from the principles of open justice. Further the application of common law powers for the court to sit in private in the *Incedal*[486] case and also in *R v Abdallah* … have been controversial and have given rise to concerns.[487]

7.93 Peters and Peters stated:

> We agree that such a review ought to be undertaken. However, we note that a direct comparison with the relevant civil law procedure (as mooted in the Consultation Paper) may be misleading inasmuch as the "closed material procedure" is aimed at withholding material from the non-governmental party to a civil case, as opposed to hearing sensitive material in camera. In our view, withholding material from another party in a criminal case is squarely against the right to a fair trial and thus should be preserved for the most extreme of circumstances.[488]

7.94 Other consultees, including the National Union of Journalists,[489] Professor Woods, Dr McNamara and Dr Townend, Guardian News and Media and the News Media Association were concerned that any review would inevitably lead to further restrictions on open justice.

7.95 Professor Woods, Dr McNamara and Dr Townend expressed the view that the Justice and Security Act 2013 "is not concerned with open justice; it dispenses with it", instead focusing on the effective administration of justice. They added that the Act is "highly contentious and there is great dissatisfaction with its approach that denies a party to the case access to relevant information …". They stated:

> The suggestion in the consultation paper that such [civil] powers should be extended to the criminal context should be not be pursued. Moreover, there is no good reason at this point in time to embark on a wider review of criminal trial process and national

---

485 Bar Council and Criminal Bar Association, para 68.

486 *Guardian News and Media Ltd v R & Erol Incedal* [2016] EWCA Crim 11; [2016] 1 WLR 1767.

487 BBC, p 7.

488 Peters and Peters, p 14.

489 The National Union of Journalists observed they were "opposed to any further expansion of closed courts proceedings, especially in regard to cases involving journalists and media organisations abroad": National Union of Journalists, p 3.

> security issues. The *Incedal*[490] case is presently and should hopefully remain an exceptional one. … We disagree with this provisional conclusion in the strongest possible terms.[491]

7.96 Guardian News and Media stated that they:

> …would not support any proposal that would result in the availability of closed material proceedings in criminal courts. There is considerable disquiet about its use in civil proceedings, and it would be wholly inappropriate to introduce it to a criminal court context.[492]

Analysis

7.97 In our Consultation Paper, we referred to closed material proceedings with the aim of highlighting that this area of the law has been subject to review in the civil context, but not the criminal. In making this point, we did not take a view as to the merits of closed material proceedings.

7.98 However, a common thread throughout a number of consultees' responses to provisional conclusion 21, was a concern regarding both the nature of closed material proceedings and any extension of them to the criminal context.

7.99 We acknowledge these concerns, but view them as relevant to a separate, albeit important, issue. We remain conscious of the need to ensure the balance between the right to a fair trial and protecting sensitive material in criminal proceedings.

Recommendation 31.

7.100 We recommend that a separate review be undertaken to evaluate the extent to which the current mechanisms in the criminal trial process strike the correct balance between the right to a fair trial and the need to safeguard sensitive material.

---

490 *Guardian News and Media Ltd v R & Erol Incedal* [2016] EWCA Crim 11; [2016] 1 WLR 1767.

491 Woods, L McNamara and J Townend, paras 5.1 to 5.6.

492 The Guardian, p 75.

PART III

Public Interest Disclosures

Chapter 8: An Introduction to Public Interest Disclosure

INTRODUCTION

8.1 The purpose of this chapter is to introduce the final part of this Report, concerning public interest disclosures.

8.2 The public interest in national security and the public interest in transparent, accountable government are often in conflict. While, no doubt, public accountability can ensure that government is protecting national security, the relationship between security and accountability is nonetheless one of tension. Effective protection of our national security relies on laws of confidence and secrecy. Used well, these laws protect our democracy, our economic well-being, and our lives; we sacrifice a portion of our liberties in order to ensure that we have any liberties worth sacrificing. Abused, these laws allow wrongdoing to flourish – for states to place themselves beyond the reach of the law – and so undermine the very democracy their creation sought to uphold.

8.3 Our concern in this part of the Report is to reconcile these competing interests (so far as possible). It is to propose a legal model that ensures that the price of protecting national security is not to undermine the rule of law (and vice versa). We are concerned to ensure that those with evidence of wrongdoing in Government do not feel that they must commit a serious criminal offence and take the law into their own hands, risking both the national security and people's lives, in order to have that evidence properly investigated.

8.4 The chapters that follow consider:

(1) The UK's obligations under Article 10 of the European Convention on Human Rights ("ECHR"), protecting the right to freedom of expression;

(2) our recommendation for a statutory commission to receive evidence of serious wrongdoing, where disclosure of that matter may otherwise constitute an offence under the Official Secrets Act 1989 ("OSA 1989"). That commission will effect meaningful investigation and, where appropriate, redress of the complaint in accordance with the public interest;

(3) our recommendation to introduce a public interest defence to offences under the OSA 1989. This will allow those prosecuted for unauthorised disclosures under the OSA 1989 to argue that their disclosure, taken as a whole and considering the manner of disclosure, was in the public interest (bearing in mind that the public interest extends not only to propriety in government but also to national security).

8.5 These recommendations follow extensive consideration of the responses to our Consultation Paper, as well as an analysis of domestic jurisprudence and of the jurisprudence of the European Court of Human Rights ("ECtHR"). We have concluded

that we cannot be certain that the current legislative scheme, in the OSA 1989, affords adequate protection to Article 10 rights under the ECHR. We therefore recommend the creation of a statutory commission to ensure adequate protection to public interest disclosures for the purposes of Article 10 and domestic law. Such a commission also reflects the broader principle that the cloak of confidentiality should not be used to mask serious wrongdoing.

8.6 We consider that there may be rare cases when the statutory commission that we recommend would not constitute an effective investigative mechanism for the purposes of Article 10. There will be exceptional cases in which the disclosure is made by a Crown Servant or other official caught by the OSA 1989 when the commission cannot provide an effective response (eg through pressure of time or because it is itself conflicted). Such a commission would also not operate effectively in the case of a journalist or other citizen who is in possession of material protected by the OSA 1989. We therefore also recommend a public interest defence which would be available to those charged with offences under the OSA 1989.

8.7 We discuss Article 10 in detail in the following chapter.

8.8 In this Part, we draw distinctions between public servants (ie those subject to section 1-4 of the OSA 1989 – Crown servants, government contractors and notified persons) and civilians (ie those subject to sections 5 and 6 of the OSA 1989). This is because different considerations apply when assessing the extent of their right to freedom of expression under Article 10 ECHR (or, more accurately, the extent of the state's discretion to interfere with that right). Of particular note – and this is a point highlighted in much ECHR case law – is the duty of loyalty owed by public servants to their democratically elected government. There is a clear public interest in governments being able to rely on their public servants. This is not a duty that applies in the case of civilians. Indeed, with certain civilians – such as journalists or academics – the duty arguably points in the opposite direction: there is a clear public interest in government being held to account.

8.9 The analysis that follows is our assessment of the law and what we believe it practically requires. What the law requires is, given the above, different depending on whether the person disclosing official information is a public servant or a civilian. Our position is not, however, that this distinction must forever be maintained: as we note in Chapter 11, Parliament may choose to legislate in such a way as to go *beyond* what ECHR law requires. That, however, is a political matter. What we present is a mechanism for ensuring we comply in all cases with the legal demands of Article 10.

THE STRUCTURE OF THIS PART OF THE REPORT

8.10 In this chapter, we will consider consultees' responses to our questions on public interest disclosure generally in our Consultation Paper. These responses were helpful in shaping our views. The many useful submissions have been taken into account when forming our recommendations. They provide the context for understanding some of the rationale behind the recommendations in the following chapters. The Consultation Paper was never intended to be, nor was it, our final view on the various matters under consideration.

8.11 First, we consider the consultation responses in respect of our proposals for a statutory commissioner. Our position in the Consultation Paper was that a statutory commissioner was necessary because the existing channels for making authorised disclosures would not at all times constitute an effective mechanism for investigating concerns of wrongdoing. We continue to see the benefit of a statutory commissioner model and make recommendations in Chapter 10.

8.12 Secondly, we consider the responses to our questions in respect of a public interest defence. We presented a number of concerns in our Consultation Paper relating to the introduction of such a defence, and were keen that consultees were able to provide considered answers to these concerns. Though we were aware that there were advantages in a public interest defence, we provisionally concluded that those advantages were outweighed by the disadvantages. As will be seen from the below responses, consultees have provided some helpful feedback which, combined with our analysis of Article 10 and further legal examination, has meant that we are now satisfied that the advantages outweigh the disadvantages. We recommend that a public interest defence be enacted in the OSA 1989.

8.13 It is worth noting that some consultees were reluctant to support a statutory commissioner model on the basis that it lacked a public interest defence as a backstop. The model we have proposed addresses this concern.

OUR APPROACH IN THE CONSULTATION PAPER TO THE STATUTORY COMMISSIONER

8.14 In the Consultation Paper we provisionally proposed a statutory commissioner to whom Crown servants and others caught by ss 1-4 of the OSA 1989 could make disclosures. One of the reasons for this provisional proposal was that we did not consider that the current regimes for receiving disclosures constitute effective investigative mechanisms[493] in respect of disclosures of confidential information, and therefore those regimes are unlikely in all situations to be compliant with Article 10 ECHR.

8.15 We begin by examining the existing regime and explain the concerns expressed to us about the efficacy of the present mechanisms by which officials bound by the OSA 1989 can raise concerns about alleged impropriety without making an unauthorised disclosure.

The Civil Service Commission

8.16 In our Consultation Paper, we examined an existing route of complaint that is available to civil servants, the Civil Service Commission. By virtue of section 9(2) of the Constitutional Reform and Governance Act 2010, a civil servant may make a complaint to the Civil Service Commission if:

(1) they are being, or have been, required to act in a way that conflicts with the Civil Service Code, or

[493] Effective, in that they are expeditious, independent, have statutory powers to compel disclosure, search powers etc.

(2) another civil servant covered by the code is acting, or has acted, in a way that conflicts with the Civil Service Code.

8.17 The Civil Service Commission has statutory powers that enable it to investigate complaints.

8.18 We noted research from Dr Ashley Savage, an academic at the University of Liverpool, showing that the number of approaches civil servants have made to the Civil Service Commission is low.[494]

8.19 Consultation question 15 stated:

> We welcome views from consultees on the effectiveness of the Civil Service Commission as a mechanism for receiving unauthorised disclosures.

Responses

8.20 Apart from Dr Ashley Savage, few consultees had first-hand experience and knowledge of the Civil Service Commission. For this reason, most consultees did not engage with this consultation question. The general view was that the Civil Service Commission would not be suited to receiving disclosures under the Official Secrets Act 1989.

8.21 Peters and Peters suggested that introducing a procedure for making anonymous disclosures to the Commission could encourage disclosures and thus reduce external leaks.

8.22 In a detailed answer, Dr Ashley Savage stated:

> These disclosures are currently 'authorised' by the Official Secrets Act 1989. The Commission also confirmed in a response to a Freedom of Information request to the author that it has procedures in place for handling such concerns. The author suggests that there is scope for the Civil Service Commission to take a more active role in the handling of whistleblowing concerns by Civil Servants. Although it is acknowledged that the Commission have made progress to introduce guidance to whistleblowers and organisations more is possible. For example, the guidance and the Civil Service Code could be clearer on when the Commission will be prepared to receive a concern. The guidance steers Servants to use internal processes only identifying that they 'may consider receiving a concern direct' this is rather vague, particularly considering that the Civil Service Commission is effectively the last official option available – at least as far as the Civil Service Code is concerned. The Code makes clear that:
>
> > "If the matter cannot be resolved using the procedures set out above, and you feel you cannot carry out the instructions you have been given, you will have to resign from the Civil Service."

[494] Para 7.83.

> The wording is unhelpful particularly because even if the Commission agrees to investigate a concern it has no power to make departments follow corrective action and can only make recommendations…
>
> …the author wishes to highlight that the Civil Service Commission is limited to investigating breaches of the Civil Service Code. The author advises the Law Commission that further consideration needs to be given to matters of concern which may fall outside of this remit.

8.23 The News Media Association were sceptical of the Civil Service Commission's effectiveness:

> Issues are not subject to outside scrutiny and debate. The Civil Service Commission retains the discretion as to whether matters are taken up with the permanent secretary, or will be included in any report to Parliament or made public in any way.[495]

8.24 The BBC stated:

> There appears to be little evidence that internal mechanisms for reporting wrongdoing are widely used or effective. Indeed, the Commission notes the very low number of approaches made to the Civil Service Commission despite it having been given statutory powers. This may be indicative of a lack of faith on the part of civil servants in whistle-blowing procedures as noted by the Public Administration Select Committee in its investigation of Whitehall leaks. We also note that there is no appeal mechanism from the Commission's decisions and no obligation on the state to follow the Commission's recommendations.[496]

8.25 Campaign Against Censorship stated:

> The Commission is ineffective because it covers civil servants only, and not others who may have access to official information in the course of their employment.[497]

8.26 Whistleblowers UK stated:

> Whilst a reasonable proposal in theory, in practice this would we believe be ineffective. Whistleblowers UK has put forward proposals for a statutory and independent Office of the Whistleblower; we are happy to share those proposals with the Commission if desired.[498]

8.27 The Bar Council/Criminal Bar Association stated:

> … there appears to be force in the expressed concerns over the fact that there is no appeal mechanism from the Commission's decisions, that its procedures are seldom

---

495 News Media Association, p 6.

496 BBC, p 11.

497 Campaign Against Censorship, by email.

498 Whistleblowers UK, pp 3 – 4.

invoked and that there is no legal obligation on the state to follow its recommendations.[499]

8.28 The Government Response stated:

> The Civil Service Commission has commented that its remit is limited to hearing appeals under the provisions of the Civil Service Code and is set out in the Constitutional Reform and Governance Act 2010. It does not receive protected disclosures nor is it a prescribed person for the purposes of the Public Interest Disclosure Act. Those concerns that are raised by civil servants and investigated in the Department, and in some cases appealed to the Commission, would not therefore be considered to be unauthorised disclosures for the purpose of the Civil Service Code. The Civil Service Code is an effective framework for civil servants (outside of the security services, and military) to raise concerns of an ethical nature and be automatically protected in doing so, with the right to refer the matter to the Civil Service Commission on appeal. The Commission does not see the possibility or any benefit in extending its scope to receiving disclosures outside of the remit of the Civil Service Code, which would require additional resource and alter its statutory remit.

Analysis

8.29 As consultees pointed out, the Civil Service Commission does not facilitate or authorise public disclosures. Information that may be disclosed to the Civil Service Commission would not necessarily fall within the scope of the Official Secrets Act 1989. If the information did not fall in scope it would therefore not be a criminal offence under the Official Secrets Act 1989 publicly to disclose this information. Were it to be publicly disclosed, the Public Interest Disclosure Act 1998 would ensure that no employment retaliation could be taken against the civil servant in question, provided the relevant statutory criteria were satisfied.

8.30 The Civil Service Commission performs a vital function by hearing appeals under the Civil Service Code and by also directly receiving complaints. But, for the reasons given by consultees, we do not consider it is an appropriate mechanism for receiving disclosures of the type we are considering in this Report. Whether the Civil Service Commission's remit should be broadened to facilitate public disclosures is a matter that we have concluded falls outside the scope of this Report. We note, however, that for many consultees this was the reason why the Civil Service Commission was seen to be inadequate as a safeguard in the official secrets context.

8.31 Our discussion in Chapter 9 highlights the need for a robust investigative mechanism. One of the reasons for that is to ensure that unauthorised disclosures are discouraged. They would be a last resort if a statutory commission were to be introduced. As it has been suggested that the current mechanism, the Civil Service Commission, appears not to be robust and wholly effective for disclosures under official secrets legislation, we have outlined in Chapter 10 the case for a statutory commissioner (and specifically the Investigatory Powers Commissioner's Office ("IPCO")) to carry out this function.

---

[499] Bar Council/Criminal Bar Association, para 95.

Existing external mechanisms

8.32 In our Consultation Paper, we noted that members of each of the security and intelligence agencies have access to an Ethical Counsellor. The role of the Ethical Counsellor has been described as follows:

> 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.[500]

8.33 In addition to the Ethical Counsellor, members of the security and intelligence agencies can take their concerns to the Staff Counsellor. The role of Staff Counsellor is fulfilled by someone who is not a member 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 enables the matter to be brought, safely, to the attention of someone who is outside the agency in question.

8.34 In our Consultation Paper, we noted that stakeholders held divergent views on the effectiveness of the Staff Counsellor as a safeguard. On the one hand, it was criticised for a perceived inability to act in an appropriately direct and urgent fashion. On the other, some stakeholders appreciated the informal nature of the Staff Counsellor model and its ability to address concerns through dialogue and explanations.[501]

8.35 There are a number of other external mechanisms for reporting concerns. First, there is the Intelligence and Security Committee of Parliament ("ISC"). Since our Consultation Paper was published, it has been confirmed to us that members of the security and intelligence services may report their concerns to the ISC. The ISC is a cross-party Parliamentary committee. As a result, it does not align itself to any one party and is independent of government.[502] Its members are nominated by the Prime Minister, but they are formally appointed by Parliament. The ISC is more autonomous than normal select committees of Parliament. However, the ISC lacks the necessary investigative powers to examine allegations of impropriety or illegality held by a concerned Crown servant which would involve an unauthorised disclosure under the OSA 1989 were the Crown servant to air them publicly. It has reasonably extensive powers to compel disclosure and oral evidence, but this form of inquiry lends itself to audit after the fact, rather than detailed on-site investigation of alleged ongoing or pending wrongdoing.

8.36 Secondly, a concerned Crown servant could make a disclosure to the Attorney General. That disclosure would be an authorised disclosure for the purposes of the OSA 1989. However, we do not consider that this could constitute an effective mechanism in all situations, given the lack of independence of the Attorney General from government. There would be a public perception problem as well as the purely

---

500 Intelligence and Security Committee, 2007-2008 Annual Report (March 2008) Cm 7542, para 66.

501 See Consultation Paper, paras 7.94 – 7.96.

502 The statutory source of the Committee's powers is the Justice and Security Act 2013. Ministers of the Crown are ineligible for membership of the ISC – though notably members must be nominated by the Prime Minister, albeit following consultation with the Leader of the Opposition (section 1(4)-(5) of the JSA 2013).

practical difficulty that the Attorney General's Office is not designed to deal with investigating such sensitive matters.

8.37 Thirdly, a disclosure to either the Director of Public Prosecutions (DPP) or the Commissioner of the Metropolitan Police Service (MPS) could be made. As noted by Lord Bingham in *R v Shayler*, 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."[503] However, it is not clear whether they would be considered effective investigative mechanisms in all situations. The DPP is appointed by and superintended by the Attorney General, and the Commissioner of the MPS is appointed by and accountable to the Home Secretary and also involved in intelligence-gathering and counter-terror policing; it is conceivable that there may be situations where their independence would be compromised. Further, they lack experience of conducting reviews and investigations within the security and intelligence services.

Proposals for a statutory commissioner

8.38 Given these potential shortcomings in the existing external disclosure mechanisms, we considered in our Consultation Paper whether a statutory post might be added as an additional, external tier, either by enshrining the existing Staff Counsellor post in legislation or by establishing an additional statutory commissioner. We felt that an additional tier would bring greater benefits and allow the Staff Counsellor's role as an informal, independent mediator to be maintained. We suggested that IPCO, which consists of the Investigatory Powers Commissioner and a number of Judicial Commissioners,[504] would be a suitable office-holder to whom members of the security and intelligence agencies could make disclosures. IPCO has the following characteristics which led us provisionally to conclude that it would provide a suitable means of receiving and addressing concerns:

(1) it has powers to investigate and require cooperation from the security and intelligence agencies;

(2) it is independent of both the security and intelligence agencies and the Government;

(3) only individuals who have been held high judicial office (ie at least High Court judges) are eligible to become Judicial Commissioners;

(4) it is intended to be more public-facing than the statutory commissioners it replaces.

8.39 The cumulative impact of these factors led us provisionally to conclude that permitting disclosures to be made to IPCO would ensure concerns about alleged wrongdoing could be effectively investigated without the risks that might be associated with

---

503 *R v Shayler* [2002] UKHL 11, [2003] 1 AC 247 at [26].

504 Judicial Commissioners are current and recently retired High Court, Court of Appeal and Supreme Court Judges. The list of Judicial Commissioners can be found here: https://www.ipco.org.uk/ (last visited 25 April 2019).

disclosing the information publicly. We also believed it would instil greater confidence in members of the security and intelligence agencies to disclose a concern than would be the case with a statutory public interest defence, as they could do so without having a detrimental impact on their career or risking prosecution.

8.40 Provisional conclusion 25 stated:

> 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?

Responses

8.41 Professor Woods, Dr McNamara and Dr Townend described this provisional conclusion as "a welcome starting point" but could not agree with it in the abstract:

> This model needs: (a) to be fleshed out more fully with some uncertainties resolved, (b) to have a pathway for former employees, and (c) accompanied by a public interest defence, as the Canadian model is.

8.42 In a detailed response, Public Concern at Work stated:

> We welcome the call for reform of the internal whistleblowing arrangements that exist in the intelligence agencies; we feel this is long overdue. We see though a major flaw in the conclusion that changes to internal arrangements on their own, even if the system creates an independent oversight mechanism, can fully replace the need for a PID…
>
> …We do though back the report's conclusions that the whole system would benefit from an additional independent oversight tier to the arrangements.
>
> We welcome the proposal to extend the Investigatory Powers Commissioner (IPC) role into being an independent oversight body for whistleblowing within the security services, as opposed to formalising in law the Staff Counsellor's role. This is something that we have also called for in our response to the Investigatory Powers Act when it went through the legislative process in 2015.[505]

8.43 Public Concern at Work made a series of helpful suggestions as to how the form and structure of this new process could be designed.

8.44 Trinity Mirror were concerned about the potential for introducing delay:

> This is an internal mechanism about which Trinity Mirror has no specific comment, but this process should not be used to prevent, or be an alternative to, whistleblowing of wrongdoing to news organizations. It is easy to envisage a system like this taking months to get through the red tape and internal procedure and the end result would be that serious wrongdoing would be kept secret or covered up by the Government. It is a matter of degree, but serious wrongdoing or gross

[505] Public Concern at Work, paras 33-37.

incompetence that is clearly in the public interest to expose should not be hidden from public view.[506]

8.45 The Courage Foundation stated that it was important that internal reporting channels were available to contractors as well as employees of the government. They found our provisional conclusion appropriate "as long as the Commissioner's workload is manageable":

> Finally, given that the Intelligence and Security Committee is also responsible for oversight of the security and intelligence services, we think consideration should be given as to whether individuals should be empowered to report their concerns to the Committee, either directly or via the Commissioner.[507]

8.46 Former intelligence officer Annie Machon stated that she would welcome the concept of an independent channel to which those with ethical concerns could turn:

> In fact an independent channel is a concept I have been publicly advocating for years… as to my mind the potential whistleblower can thereby avoid losing their career and potentially their liberty, and the intelligence agency avoids a scandal and can potentially improve its working practices and better protect the nation.[508]

8.47 ITN stated concerns about anonymity of those reporting to IPCO:

> Rather than leaking information to journalists the Law Commission suggests whistleblowers should initially raise concerns to an Investigatory Powers Commissioner, rather than a journalist. This is a woefully inadequate solution to attempt to demonstrate self-regulation. It would be impossible for whistleblowers to remain anonymous under such circumstances and in all likelihood having to alert officials to misgivings over, for example, systemic failings would be enough to put off those who wish to leak vital information altogether.[509]

8.48 The BBC expressed concerns about the capacity of the Commission to deal with matters raised effectively and expeditiously:

> As far as the proposal to utilise the Investigatory Powers Commissioner is concerned we believe that it seems disproportionate to create a new bureaucratic process and to vest powers in a, so far, untested new appointment when the departments concerned and the Courts could provide a sufficient framework as is currently the case. We also agree with the points made in paragraphs 41 to 46 of the submission of English PEN, Article 19 and Reporters Without Borders and particularly their concern that the office of the Investigatory Powers Commissioner may not have the capacity to discharge this function at speed which is essential where the information in question is time-sensitive.[510]

---

506 Trinity Mirror, by email.

507 Courage Foundation at pp 5, 15-16.

508 Annie Machon, p 2.

509 ITN Response, p 7.

510 BBC Response, p 12.

8.49 English PEN, Index on Censorship and Reporters Without Borders argued that it was difficult to evaluate the effectiveness of the Investigatory Powers Commissioner given the office had at that time only recently been established. It may not be able to address time-sensitive information sufficiently promptly. They argued that our Consultation Paper gave insufficient consideration to the need for an "ethic of transparency and dissemination of information".[511]

Analysis

8.50 Recognising some of the concerns raised by consultees, we have sought to identify the essential attributes that a statutory commission, whether the Investigatory Powers Commission or some bespoke body, must have in order to be effective. In seeking to identify these essential attributes, we have focused on the purposes the commission would serve and the functions it will fulfil. We have also drawn upon the European Court of Human Rights' comments on the minimum that can be expected for compliance with Article 10.

8.51 One effective method of holding government and its agencies to account is through oversight by an independent body. Meaningful independence means that the commissioner must have security of tenure (even if for a specified term) in order to ensure so far as possible that improper influence cannot be exerted against him or her. The perception of independence is as important as the reality: those who go to the statutory commissioner must have confidence that their disclosure will be taken seriously, and rigorously and impartially investigated by someone who is independent and not susceptible to governmental pressure. Those who have held high judicial office are best-placed to fulfil this role: they have been selected for integrity and independence and have years of experience and training in exercising independent judgment.

8.52 However, in order to be an effective mechanism for receiving and investigating disclosures (that would otherwise be unauthorised disclosures), the body would also have to be able to act in a sufficiently timely fashion. This is not only a question of statutory time-frames, but includes the practical ability to investigate all reaches of the intelligence, security and defence bodies. This would require the body to have extensive knowledge of relevant contacts and procedures. We do think that stakeholders' concerns in this area can be met. It would also be necessary for the body to have sufficient powers to be able to conduct investigations without hindrance. At a minimum, those investigating would require sufficient security clearance, as well as the legal powers to compel disclosure. Again, we consider that the body we propose can act effectively in these respects.

8.53 In our Consultation Paper, we proposed augmenting the function of IPCO to take on this role. It was our view that IPCO would be well-placed to investigate concerns of wrongdoing, given its existing jurisdiction, independence and investigative reach with respect to the UK intelligence community. As noted above, a number of consultees agreed that the UK system for disclosures would benefit from independent oversight, and many agreed provisionally that IPCO would be well-placed to undertake the role, whilst recognising that, at the time, IPCO was in its infancy. It remains our view that a statutory commissioner should form an essential part of our scheme to ensure the

[511] English PEN, Index on Censorship and Reporters Without Borders Response, pp 16-17.

UK's future compliance with Article 10. We consider that IPCO is uniquely well-suited to the task. We make recommendations in detail in Chapter 10.

OUR APPROACH IN THE CONSULTATION PAPER TO THE PUBLIC INTEREST DEFENCE

8.54 In this section, we briefly summarise the problems with introducing a statutory public interest defence which we identified in our Consultation Paper. The cumulative weight of these problems led us provisionally to conclude that the advantages of doing so were outweighed by the disadvantages. We identified three key problems that could potentially follow should a statutory public interest defence be introduced:

(1) the potential to undermine the relationship of trust between ministers and civil servants;

(2) the potential risk to others and to national security; and

(3) the inherently uncertain nature of the concept of public interest, which has the potential to impact on the criminal justice system as a whole, including by encouraging disclosures that are wrongly believed to be in the public interest.

8.55 Some consultees examined each of the potential problems we raised. Others made valuable comments of a more general nature, including suggestions that we had undervalued the benefits of a public interest defence. We consider all of these in the following sections. Finally, we include a brief discussion of the effect that a public interest defence might have on principles of open justice.

Responses of a general nature

8.56 The Crown Prosecution Service agreed with our analysis and the potential problems we identified. The Government Response also agreed, stating:

> We continue to believe that the reasons for not introducing a public interest defence given in the White Paper that preceded the Official Secrets Act 1989 remain valid. Further, we do not believe that the introduction of such a defence would in fact bring any tangible benefit to the public interest, given the means that already exist to hold the security and intelligence agencies to account and ensure that misconduct and impropriety can be brought to light and dealt with.

8.57 Prof Jacob Rowbottom submitted that there was a strong case for enacting a public interest defence. This was based on his analysis of the limitations of relying exclusively upon internal government reporting mechanisms to address concerns. Prof Rowbottom stated:

> An internal safeguard may be appropriate for certain types of concern, while a right to go public may be appropriate in others. For example, where a member of the security and intelligence services wants to report some misconduct by a colleague, the internal system may be an appropriate way for such complaints to be investigated and for remedial action to be taken. However, in other cases a whistleblower may not wish to report some wrongdoing that requires corrective action, but seek to disclose information that the public has a right to know in order to assess the actions of government. For example, a decision to supply military

equipment to a particular country or to covertly monitor certain communications may not be the type of wrong that an internal process can deal with (if it is part of a strategy approved by government), but there is an argument that the public should know these activities are taking place.

8.58 Prof Rowbottom identified a number of challenges that might be encountered in seeking to enact a public interest defence. He thought none of these were insurmountable, however. First, he recognised that there is a distinction between the subjective and objective versions of the defence. Rowbottom suggested that to minimise any risk of the defence being abused, the test should be formulated with both subjective and objective limbs. This would require the defendant "reasonably to have believed that the disclosure of the information was in the public interest" and also that "publication of the information was in fact in the public interest".

8.59 Secondly, Rowbottom asked how a public interest defence would deal with the issue of mass disclosures of information, the release of only some of which may have been in the public interest. He stated that such "mass disclosure would inevitably go beyond that which is strictly necessary to inform people on public interest matters", but argued that if this were considered to be "fatal to a public interest defence, then some of the most important media stories would not be protected". Rowbottom suggested that certain procedural requirements could be implemented – such as participation in the Defence and Security Media Advisory ("DSMA") Notice system[512] – that, if met, could enable journalists to rely on a public interest defence in these situations. We also consider that IPCO is well-placed to meet any challenges posed by mass disclosure.

8.60 Oliver Butler, then a PhD candidate at Emmanuel College, Cambridge, agreed in principle, but stated:

> The absence of a public interest disclosure defence for officials is only acceptable if there truly are robust and effective and independent internal mechanisms to review official action and other exemptions for reporting criminality to the police.[513]

Insufficient attention to the benefits of a public interest defence

8.61 Many consultees argued that our Consultation Paper underemphasised the benefits of introducing a public interest defence, and in particular its value in protecting the role of the media in holding government to account. For example, CPU Media Trust stated:

> …public exposure can have a positive, and unparalleled, cleansing and disinfecting effect on officialdom, which only an unfettered media can deliver. The press is uniquely placed to provide the oxygen of publicity that alerts people to risk, keeps the electorate informed and holds government to account, in a way that ethics counsellors in closed backroom sessions never could…[514]

---

512 The DSMA Notice System is a means of providing advice and guidance to the media about defence and security information, the publication of which would be damaging to national security. The system is voluntary, it has no legal authority and the final responsibility for deciding whether or not to publish or broadcast rests solely with the editor or publisher concerned.

513 Oliver Butler, p 12.

514 CPU Media Trust response, pp 5-6.

8.62 The Society of Editors stated:

> We do not feel sufficient attention has been paid to the merits of an essential public interest defence…[515]

8.63 Liberty argued that national security was "strengthened by robust accountability and appropriate transparency" because errors would be corrected and wrongdoing remedied:

> Recognising the fact that large organisations – such as the UK's intelligence and security agencies – will suffer from organisational blindspots and systemic errors does not require any special scepticism towards them, just a recognition that sometimes only outside oversight – often by the press and public – can break through entrenched practice.[516]

8.64 Whistleblowers UK stated:

> The availability of a statutory public interest defence is essential, however inconvenient that may be for the authorities and/or the prosecution.[517]

8.65 Public Concern at Work stated:

> We strongly disagree with the report's [sic] conclusions in this area, and see the introduction of a public interest defence (PID) as a vital reform to ensure there is effective accountability in this sensitive area of Government activity. An absence of a PID risks undermining internal whistleblowing arrangements across Government, from Whitehall to the intelligence services, pushing concerned civil servants into making anonymous disclosures to the media.[518]

Analysis

8.66 We agree with consultees that accountability is fundamental to a well-functioning democracy.[519] This must be balanced against the need to protect sensitive information. Jacob Rowbottom neatly summed up the issue we are grappling with in the following terms:

> Everyone accepts that some government information must remain secret. The system of secrecy, however, requires safeguards to ensure that the power to withhold information is not abused to shield government from criticism or embarrassment, or to cover up wrongdoing.

8.67 In the context of official secrets legislation, the UK has historically relied upon safeguards which are "internal" to Government. As we discussed in our Consultation Paper, if a member of the security and intelligence agencies has a concern that

---

515 Society of Editors, para 26.

516 Liberty Response, p 30.

517 Whistleblowers UK response, p 3.

518 Public Concern at Work, para 23.

519 Many individual consultees were of the view that having a public interest offence was essential to the functioning of democracy, including Douglas Green, David Goepel, Susan Jackson, and Damien Shannon.

relates to his or her employment, they can approach their organisation's Ethics Counsellor. If they would prefer to approach someone who is external to the agency or department in question, they can approach the Staff Counsellor. This office is typically held by someone who is a former senior civil servant. In addition to these individuals, as noted in a letter we received from The Rt Hon Dominic Grieve QC MP, members of the security and intelligence agencies can now also bring any concerns they might have to the Intelligence and Security Committee of Parliament ("ISC"). Finally, there are legal routes that can be pursued in appropriate cases, such as by bringing a claim in the Investigatory Powers Tribunal. However, as noted above, these existing mechanisms have also been criticised as being ineffective (and the IPT, while effective in respect of its remit, is only available to victims of unlawful action by a public authority using covert investigative techniques).

8.68 In addition, these are not, in general, mechanisms which facilitate information being brought into the public domain. The ISC now constitutes an important exception, however, as it is independent of government and it publishes its findings in open reports. For this reason, the ISC represents a valuable addition to the mechanisms which have historically existed. We discuss in chapter 10 how these mechanisms could be made more robust through the addition of a statutory commissioner.

8.69 The fundamental point that many consultees made in their responses is that in a legal system which has legislation criminalising the unauthorised disclosure of certain categories of information, the only way to ensure that this legislation is not used to cover up wrongdoing is to provide a statutory public interest defence which goes beyond any internal mechanisms that exist or that can be created. No matter how robust the internal mechanism that is available, there are some matters that should, it is argued, be raised in public to expose the nature and/or extent of the governmental wrongdoing. The example given by many consultees of an unauthorised disclosure that was in the public interest was the information about the extent of state surveillance that Edward Snowden provided to the New York Times and the Guardian Newspaper in 2013. Many consultees argued that even though Mr Snowden may have committed criminal offences under the law of the United States by disclosing this information, it was in the public interest for him to have done so, as doing so revealed information that the public had a right to know. We make no comment on these disclosures, beyond noting that similar activity in this country could be an offence under the Official Secrets Act 1911 as well as the OSA 1989. Nonetheless, we follow the more general point being made by consultees in respect of a public interest defence for the OSA 1989 offences.

8.70 There is a recent example in the domestic context that only occurred after we published our Consultation Paper. In its report *Detainee Mistreatment and Rendition: 2001-2010* the ISC concluded that whilst there was no evidence to suggest that UK personnel were directly involved in the mistreatment of detainees, there was evidence to implicate some personnel in mistreatment that was carried out by others. The availability of a public interest defence might have led to this information being brought to light sooner.

8.71 Of course, the mere fact of some information being in the public interest will not, in and of itself, mean that the disclosure taken as a whole was in the public interest. As

we discuss below, any reasonable assessment of whether a disclosure was in the public interest will necessarily pay heed to the damage risked by such disclosure.

Trust and loyalty of civil servants

8.72 The Civil Service Code asserts the core values of the Civil Service as honesty, integrity, impartiality and objectivity. The Civil Service Code states that civil servants must act in a way which deserves and retains the confidence of ministers. It also states that civil servants should not disclose information without authority. In our Consultation Paper we made the point that the introduction of a public interest defence had the potential to undermine the relationship of trust and loyalty between civil servants and their ministers. A public interest defence would permit a civil servant to arrive at his or her own conclusion as to whether it was in the public interest to disclose information that could be in contravention of both the Civil Service Code and the criminal law.

8.73 This issue has been explored in detail in some recent academic literature. For example, Eric Boot has suggested:

> …the obligation to respect the democratic allocation of power prohibits civil servants from whistleblowing. The idea is that whistleblowers usurp the power to decide what is and what is not a legitimate state secret, whereas this is properly the prerogative of democratically elected officials. These officials have received a mandate from the people to decide, among many other things, on matters of state secrecy, whereas those engaged in whistleblowing have been elected neither by the people nor by its representatives.[520]

8.74 In support of his analysis, Boot cites Sagar, who argues:

> When unauthorized disclosures occur, vital decisions on matters of national security are effectively being made by private actors, an outcome that violates the democratic ideal that such decisions should be made by persons or institutions that have been directly or indirectly endorsed by citizens.[521]

Responses

8.75 It is fair to say that many consultees did not find this objection to the introduction of a public interest defence to be very compelling. For example, the Society of Editors could see no merit in the argument:

> We … do not accept the assertion that [a public interest defence's] existence would in any way undermine the trust upon which the relationship between ministers and the Civil Service is based.[522]

---

520 E R Boot, "No Right to Classified Public Whistleblowing" (2018) 31(1) Ratio Juris 70, 77.

521 Rahul Sagar, *Secrets and Leaks: The Dilemma of State Secrecy* (Princeton NJ: Princeton University Press 2013) p 114.

522 Society of Editors Response, para 26.

8.76 The Institute of Employment Rights argued that our Consultation Paper had focused on the wrong civil service value, and that disclosures should be understood as an essential part of a civil servant's role:

> Impartiality is a core value in the Civil Service Code, but disclosures in the public interest do not threaten impartiality as they are not a political act. Further, integrity is also a value in the Code and it can be argued that civil servants in serving the public interest, and holding Government to account for wrongdoing, are performing a constitutional role, rather than a political one in merely maintaining a political party in power.[523]

8.77 Liberty similarly objected:

> It cannot be right that civil servants justify the concealment of serious wrongdoing using a cloak of Ministerial trust. Certainly, only disclosures the revelation of which is in the public interest should be protected. The threat of prosecution and imprisonment for disclosures which are not so justified will remain a powerful deterrent. But trust in a civil servant not to reveal blatant illegality is not something to be fostered, but opposed.[524]

8.78 The Courage Foundation made the point that civil servants are already obliged to ensure Parliament is not misled.[525] CPU Media Trust argued that disclosure in the public interest must "trump misplaced loyalty" when "required to cover up mismanagement, misconduct or malpractice".[526]

8.79 The Campaign for Freedom of Information/Article 19 criticised the focus on "trust":

> The preservation of 'trust' had long been the justification for retaining the discredited section 2 [of the Official Secrets Act 1911], criminalising the unauthorised disclosure of *all* official information. If the current proposals are based on the need to protect trust between ministers and officials, ministers in the Department of Transport, the Department for Education, the Department for Work and Pensions and others may argue that they have as much need as their Foreign Office or Ministry of Defence colleagues for their officials' loyalty. This would point to a return to the philosophy of the old section 2.[527]

8.80 Public Concern at Work made the important point that the way in which a public interest defence was drafted would make a critical difference to the risk it posed:

> A poorly drafted PID could create this risk but this can be mitigated by ensuring that the drafting of the defence so safeguards minimise [sic] the risk of damage to public security. This issue has already been considered in depth by Principle 43 of the

---

523 Institute of Employment Rights Response, p 10.

524 Liberty Response, pp 26-27.

525 Courage Foundation, p 14.

526 CPU Media Trust Response, p 6.

527 Campaign for Freedom of Information/Article 19 Response, p 14. Emphasis in original.

> Tshwane Principles [which] provides examples of safeguards that courts and juries could be required to consider when applying the defence…[528]

Analysis

8.81 There is no doubt that members of the security and intelligence agencies and civil servants more generally should not attempt to cover up wrongdoing or mislead others. This is clearly set out in the Civil Service Code. There are various channels within the Civil Service that enable civil servants to raise a concern with the option of eventually bringing it to the attention of the independent Civil Service Commission.

8.82 The responses provided by consultees reveal a tension that has a bearing on the amorphous nature of the concept of "public interest". Some consultees took the view that a disclosure would be justified on the basis that it was made with the intention of uncovering "mismanagement, misconduct or malpractice". Others, however, expressed the view that a disclosure would be justified if it revealed "serious wrongdoing". We will return to this issue when we discuss the inherent uncertainty of the concept of public interest below. In any event, any public interest defence would have to recognise the need for respect and trust between civil servants and ministers (and, indeed, between public servants generally).

Risk to others and national security

8.83 A public interest defence might encourage someone to disclose information without authorisation on the basis that he or she genuinely believes that it is in the public interest to do so. One of the points we made in our Consultation Paper was that the individual in question may not have all the information necessary to evaluate accurately whether making the disclosure would in fact be in the public interest. This problem was neatly summed up by Lord Hope in the following terms:

> 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.[529]

8.84 When a civil servant discloses information contrary to the Official Secrets Act 1989, he or she may take the view that the potential risk to national security is outweighed by the public interest in disclosing the information in question. Even where a public interest defence would be available, the civil servant has no way of knowing whether a jury will ultimately agree with his or her assessment of what the public interest permits, or whether they will be convinced by the arguments advanced by the prosecution. Should the jury disagree, the civil servant will be convicted if the prosecution can adduce evidence to persuade the jury that the harm caused or risked by the disclosure meant that it was not in the public interest to make it. This possibility, as we have explained earlier, suggests that were a public interest defence to be introduced, it might need to be drafted in such a way that it provides guidance to both civil

---

528 Public Concern at Work, para 29.

529 *R v Shayler* [2002] UKHL 11, [2003] 1 AC 247, para 84.

servants and juries as to what is, and potentially what is not, in the public interest. We return to this issue below.

Responses

8.85 Most consultees saw little merit in this concern. They argued that weighing up the public interest in disclosing the information against the potential impact to national security was the very essence of a public interest defence. CPU Media Trust stated:

> [The potential risk to national security] is an inherent risk for the security services, but any public interest defence should be judged on whether the benefit of the disclosure was proportionate to the risk.[530]

8.86 The Institute of Employment Rights accepted that introducing a public interest defence brought an increased risk to national security but argued that it should not be used as a "cloak for impropriety, illegality or wrongdoing on the part of Government". It was argued that there was a need to balance the interests involved.[531]

8.87 In their responses, Liberty and English PEN/Reporters without Borders/Index on Censorship were critical of the references to "mosaic theory" in our Consultation Paper. Mosaic theory has been described by Professor Pozen as the process by which:

> 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.[532]

8.88 There are three dimensions to this process. First, the defendant may not necessarily have access to all relevant information – the "full picture". The information they disclose may, combined with other information unknown to the discloser, be detrimental to the safety and security of others or to national security to a degree or in ways which the defendant could not have predicted. Secondly, the jury will not know the "full picture" at trial in assessing whether or not the disclosure was made in the public interest. Thirdly, it is arguable that revealing the "full picture" at trial may mean that wider damage may be done by others who piece together material gained from the trial. 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.[533] 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.

---

530 CPU Media Trust, para 4.4.

531 Institute of Employment Rights Response, p 10.

532 D Pozen, "The Mosaic Theory, National Security, and the Freedom of Information Act" (2005) 115 Yale Law Journal 628, 630.

533 D Pozen, "The Mosaic Theory, National Security, and the Freedom of Information Act" (2005) 115 Yale Law Journal 628, 650 and 678.

8.89 English PEN, Reporters Without Borders, and Index on Censorship were not persuaded by this argument, and commented that we did not mention Pozen's description of mosaic theory as "undertheorized and prone to misuse":

> [we] submit that the consideration of the impact of 'mosaic' theory of national security risks ought not to form any part of the assessment of a public interest defence to disclosure offences.[534]

Analysis

8.90 As a preliminary point, it is worth emphasising that a public interest defence may require the prosecution to put evidence before the jury to demonstrate why the disclosure was not – despite the defendant's assertions – in the public interest. Under the current law, the prosecution does not need to prove that the defendant's unauthorised disclosure caused specific damage. This is the case not only for the offence contained in section 1(1) of the Official Secrets Act 1989, but also for those offences which include a damage element. In the case of those offences which include a damage element, it is sufficient for the prosecution to prove that the information disclosed by the defendant was such that its unauthorised disclosure would *be likely to* cause damage.

8.91 If the defendant seeks to argue that the unauthorised disclosure was in the public interest, the defence will point to the benefits the disclosure had even though it may have been likely to result in damage. To rebut the defendant's contention that the unauthorised disclosure was in the public interest, the prosecution may put before the jury compelling evidence of the damage that was caused or was likely as a result of the civil servant's unauthorised disclosure. That disclosure by the Crown of more specific details as to the damage will compound the damage in fact risked or caused by the unauthorised disclosure in the first place. In many cases the Crown may choose not to adduce such evidence and the prosecution would either fail or, in anticipation of this, not be brought in the first place.

8.92 Where such evidence is adduced this could in some cases increase the chances of a conviction, given the impact such evidence may have on the jury. The availability of a public interest defence may counter-intuitively therefore increase the prosecution's chances of securing a conviction over and above the position under the present law, given that the prosecution is not currently required to reveal the specific damage that was caused. We discuss later in this section the impact on the trial process of the prosecution having to place evidence before the jury to demonstrate why the disclosure was not in the public interest.

8.93 Further, we do not doubt that mosaic theory, taken to an extreme, could be used as the justification for a wholly disproportionate level of restriction and censorship. However, this does not mean that the theory is without basis. Undertheorized it may be, but

534 English PEN/Reporters Without Borders/Index on Censorship, para 37.

> the theory's basic premise is valid, if simple: Informational synergy does exist, and adversaries can capitalize on it to our detriment. Indeed, the only way adversaries can capitalize on information disclosure is through mosaic-making.[535]

8.94 This is one of the reasons that care needs to be exercised when trying to assess the public interest in a disclosure both before and after the fact. It is also, of course, why we recommend that in addition to a public interest defence, a statutory commissioner should be empowered to investigate concerns at a sufficiently high level of clearance to ensure that sensible, informed decisions on disclosure can be made.

A public interest defence would create legal uncertainty

8.95 A further point we made in our Consultation Paper was that "public interest" might be too uncertain a concept to form the basis of a statutory defence.

8.96 By its very nature, a public interest defence requires a member of the security and intelligence agencies or a civil servant to have the settled belief that, notwithstanding the fact it constitutes both a breach of the Civil Service Code and a criminal offence, the public interest can best be satisfied by disclosing the information in his or her possession. Even if a public interest defence were to exist, the individual in question would still be charged with a criminal offence and it would be for the jury to decide whether the individual's assessment of what the public interest permitted was ultimately correct. The person who disclosed the information could understand public interest to justify revealing "mismanagement, misconduct, or malpractice", which is quite a low threshold. The jury, however, could understand public interest to justify revealing "serious wrongdoing", which is a higher threshold. In a case such as this, the defendant would be convicted, despite the availability of a public interest defence unless the defence could be defined with great precision. This uncertainty was one of the factors which led us provisionally to conclude that the disadvantages of introducing a public interest defence outweighed the advantages.

8.97 As we note above, asking juries to weigh up an amorphous and inevitably subjective concept like "public interest" without guidance could make prosecutions unpredictable and inconsistent.

Responses

8.98 Many consultees took the view that we had overstated this difficulty.

8.99 The Courage Foundation argued:

> Courts and Juries can and do contend with the concept of the public interest in other situations. Cases involving the law of confidence, data protection or the Public Interest Disclosure Act will often involve individuals having to make this kind of judgement. It is not obvious why cases involving the disclosure of official information should be considered differently.
>
> There's also already a degree of uncertainty in Official Secrets Act cases as the Attorney General makes the decision about whether to prosecute. Furthermore, in at

[535] D Pozen, "The Mosaic Theory, National Security, and the Freedom of Information Act" (2005) 115 Yale Law Journal 628, 678.

least three cases brought under the 1989 Act – that of Katherine Gunn, Derek Pasquill and the second against Richard Tomlinson – charges have either been dropped or the prosecution has declined to offer evidence. In other words, this is a system in which public interest factors play a role and do so in a very unpredictable manner. A statutory public interest defence would likely make the system more predictable, rather than less.[536]

8.100 Associated Newspapers stated:

> Public interest tests, defences and exemptions appear across English law. They include statutory provisions concerning the disclosure or publication of information. See the public interest disclosure provisions of the Employment Rights Act; section 4 of the Defamation Act 2013; section 32 of the Data Protection Act 1998; section 55(2)(ca) of the Data Protection Act 1998 (as amended but not yet in force [at that time]). There are also numerous public interest provisions in the Freedom of Information Act 2000. There are also judicially-developed public interest defences or justifications in breach of confidence and copyright.[537]

8.101 The Bar Council and CBA's response in relation to jury assessment was that:

> It is submitted that it is wrong to state that it would be "impossible" for a jury to reach a just conclusion when evaluating a public interest defence (paragraph 7.52). No empirical studies or academic opinion is cited to support the proposition. The issue of whether a disclosure is made in the public interest would be determined on an assessment of the relevant evidence which would be called and challenged. It should not be elevated into a special category of evidence. It is the experience of criminal practitioners that jurors routinely grapple with technical and complicated concepts relating to financial, medical and scientific evidence in circumstances where experts disagree. Parliament could prescribe categories of behaviour or circumstances, of which disclosure would be in the public interest; see for example Section 43(B)(1) Employments Rights Act 1996 at paragraph 7.19 and below. Although the statutory whistle blowing provisions do not apply to members of the security and intelligence services and military personnel (paragraph 7.22), they do otherwise apply to those in the employment of the Crown, who are and will continue to be subject to the OSAs and any replacement statutory regime.

8.102 The Bar Council and Criminal Bar Association also argued:

> It is not accepted that a public interest defence will inevitably offend against the certainty rule (paragraph 7.50 et seq). The requirement, in respect of the ingredients of an offence, is "for sufficient rather than absolute certainty ... no-one should be punished under a law unless it is sufficiently clear and certain to enable him to know what conduct is forbidden before he does it". Different considerations may apply between ingredients of an offence and a statutory defence and again depending on whether the defence imposes an evidential or legal burden on the defendant. The

---

536 Courage Foundation, p 15.

537 Associated Newspapers, para 16.

defence could be subject to further statutory definition, for example setting out relevant categories as per the whistle blowing provisions (see paragraph 7.19).

8.103 We received a very helpful response from English PEN / Index on Censorship / Journalists Without Borders that set out different ways the concept of "public interest" could be defined in statute. We consider this further in the next chapter, which sets out some possible models which a public interest defence could follow.

Analysis

8.104 We agree with consultees that the concept of "public interest" is one that is familiar to English law in specific contexts. As consultees pointed out, the concept is used in various statutes, such as of the Defamation Act 2013, the Public Interest Disclosure Act 1998, and the Freedom of Information Act 2000. These are all statutes that deal with the civil law. The issue we were considering in the Consultation Paper is whether a public interest defence should be available in respect of conduct that would otherwise amount to a criminal offence. The distinction between civil law and criminal law is important. As we discussed earlier in this chapter, the social benefit of the defendant's conduct is not something with which a jury is often required to grapple. As consultees pointed out, however, there are some notable examples.

8.105 Section 55 of the Data Protection Act 1998 contained a criminal offence of unlawfully obtaining, disclosing, procuring, or retaining personal data. Section 78 of the Criminal Justice and Immigration Act 2008 inserted a new defence into 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.

8.106 Section 55 of the Data Protection Act 1998 has been replaced by section 170 of the Data Protection Act 2018.[538] This provision provides that:

> (2) It is a defence for a person charged with an offence under subsection (1) to prove that the obtaining, disclosing, procuring, or retaining –
>
> (c) in the particular circumstances, was justified as being in the public interest.

8.107 Section 50 of the Serious Crime Act 2007 contains a "defence of acting reasonably", such that (under subsection (1)) a person will not be guilty of the offence of encouraging or assisting an offence if he proves –

> (a) that he knew that certain circumstances existed; and
>
> (b) that it was reasonable for him to act as he did in those circumstances.
>
> …
>
> (3) Factors to considered in determining whether it was reasonable for a person to act as he did include –

[538] See discussion at 6.27.

(a) the seriousness of the anticipated offence…

8.108 Therefore, requiring the jury to consider the potential damage or benefit of an act, while rare, does have precedent in law.

A public interest defence might "open the floodgates"

8.109 A further potential problem we identified with introducing a public interest defence is that it could encourage civil servants to make unauthorised disclosures.

Responses

8.110 Consultees submitted that we underestimated and undervalued the deterrent effect of the personal cost associated with making unauthorised disclosures. Some consultees also pointed out that we had failed to consider the role the media play in filtering and curating unauthorised disclosures. It was argued that these factors reduced the likelihood that introducing a public interest defence could "open the floodgates".

8.111 Prof Rowbottom acknowledged the danger that a public interest defence could encourage leaks where people have a genuine but mistaken belief in a public interest, but argued that it should be placed in the context of the risks they would face:

> A person would not know in advance whether a defence is likely to succeed or not. The source would likely find that the chances of success are slim, given that the courts will show considerable respect for the government's assessment of where the public interest lies. These factors would be likely to have a deterrent effect on a would-be leaker. A further deterrent would be the various adverse consequences of being identified as a leaker, aside from criminal liability, which might include the loss of employment or at least discipline at work. Rather than providing a green light for individuals to publish vast amounts of information, there is a good chance that a public interest defence will be a disappointment to those seeking greater transparency in government. The risk of a public interest defence legitimating reckless or misguided disclosures may be less significant than might initially appear.[539]

8.112 A number of other consultees, including the Courage Foundation, Compassion in Care and Campaign for Freedom of Information/Article 19 made similar points.

8.113 The Bar Council/Criminal Bar Association felt the "floodgates" argument in our Consultation Paper was "overstated" and argued that:

> In respect of the defence pursuant to Section 55 of the Data Protection Act 1998, stakeholders have confirmed that the defence is pleaded very rarely (paragraph 7.12). Whilst there is often likely to be some causal link between disclosure and the existence of a public interest defence that will not always be the case, for example where financial reward is the motivation for the disclosure. The limited empirical evidence from Canada and Denmark – jurisdictions which have enacted a public

[539] Jacob Rowbottom, para 16.

interest defences in official secret cases – suggest that it will only be rarely, if at all, where the need will arise for reliance on the defence.[540]

8.114 Media consultees tended to focus on the role they play in filtering and curating content. For example, Guardian News and Media stated:

> On the Snowden revelations, we note our role as careful facilitators, curators and moderators. During that reporting, Guardian staff took every decision very carefully. In nearly four months they published a handful of stories about GCHQ, and not a single GCHQ document in full - they quoted small portions of documents. In total, they published less than one per cent of the material they received.[541]

8.115 Similarly, The Trinity Mirror stated:

> There will be no "floodgates" effect of increased disclosure because an editor will still have to consider whether there really is a public interest about what is being disclosed and there still may be offences that it would be difficult to avoid and thus prevent publication such as the Computer Misuse Act 1990. In any event the DSMA [notice committee] is still an effective filter for what is acceptable and what is truly harmful.[542]

Analysis

8.116 Consultees were right to highlight the personal cost that those who make unauthorised disclosures will often face. The decision to disclose information without authorisation and in contravention of the criminal law is unlikely to be one that is made lightly. We find Prof Rowbottom's points about the potential impact of introducing a public interest defence compelling. It is not necessarily the case that a public interest defence will increase the likelihood of information being disclosed. It is simply impossible to say one way or the other.

8.117 Even if enacting a public interest defence does encourage civil servants to disclose information in violation of the criminal law because they believe that it is in the public interest to do so, this does not necessarily mean that the civil servant will secure an acquittal. As we have already discussed, a public interest defence may leave the person who disclosed the information no better off, because of the possibility that the jury will disagree with the accused's assessment of what the public interest permitted.

8.118 In relation to the point that was made about the role played by the press, we accept that the press can act as a filter, and that they have experience in employing their own judgement in determining what, on the basis of the information they have in their possession, might be in the public interest. Nonetheless, even to the extent that this might conceivably be some form of safeguard of the public interest, an individual who seeks to make a disclosure in contravention of the criminal law might choose not to turn to the media. He or she could decide to self-publish the material for any reason

---

540 Bar Council and Criminal Bar Association, para 87.

541 Guardian News and Media pp 2 -3.

542 Trinity Mirror, by email.

(perhaps, say, in order to increase the likelihood of remaining completely anonymous and thereby avoiding the risk of prosecution).

Open justice

8.119 We did not address the impact that a public interest defence might have on the principle of open justice in our Consultation Paper. However, it is an issue which merits consideration in any future debate, and we think it worth setting out here (see also our discussion of open justice in Chapter 7).

8.120 Open justice is a fundamental constitutional principle. In *Attorney General v Leveller Magazine Ltd* Lord Diplock said:

> As a general rule the English system of administering justice does require that it be done in public. 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.[543]

8.121 It is possible for a court to depart from the principle of open justice and to exclude members of the public, including representatives of the media, from parts of the trial (or, exceptionally, from the entire trial). As Lord Thomas CJ stated in *In re Guardian News and Media Ltd*, such a course can only be taken if it is "strictly necessary" and is the only way to ensure that justice can be done.[544]

8.122 It is for the court to determine on this very strict test whether the detailed reasons that have been advanced (for example, on the basis of national security) necessitate a departure from the fundamental principle of open justice. In practice, the Secretary of State will issue a certificate detailing the detrimental impact to national security that would follow should the evidence be heard in public.[545] This is not determinative, since, as Lord Thomas CJ confirmed, it is for the court to decide whether the reasons given by the Secretary of State are sufficiently compelling to justify abrogating the fundamental principle of open justice.[546]

8.123 A court's ability to order that parts of the trial be heard in private is augmented by its ability to order reporting restrictions, which prohibit certain matters from being reported by the media. These are subject to similarly strict conditions. Lord Burnett CJ stated in *R v Sarker* that:

---

543 *Attorney General v Leveller Magazine Ltd* [1979] AC 440, [1979] 2 WLR 247 p 449-450.

544 *In Re Guardian News and Media Ltd and others* [2016] EWCA Crim 11, [2016] 1 WLR 1767 at [73].

545 *In Re Guardian News and Media Ltd and others* [2016] EWCA Crim 11, [2016] 1 WLR 1767 at [45] – [47].

546 *In Re Guardian News and Media Ltd and others* [2016] EWCA Crim 11, [2016] 1 WLR 1767 at [51] – [52].

> reporting restrictions orders are … exceptional, require clear justification and should be made only when they are strictly necessary to secure the proper administration of justice … they are measures of last resort…[547]

8.124 Should the government agree with our recommendation to introduce a public interest defence, in future the prosecution would be compelled to put sufficient evidence before the jury to prove to the jury why the unauthorised disclosure was not in fact in the public interest. Such evidence may be of an extremely sensitive nature. If the prosecution does decide to rely upon evidence of this nature, it may apply to the judge for parts of the trial to be heard in private. Assuming the judge grants this application, this would have a detrimental impact upon open justice and could lead to less media scrutiny of key aspects of the trial. Should our recommendation be followed, careful consideration must be given to its impact upon open justice.

CONCLUSION

8.125 It is clear to us that there is a need for an external, independent body to receive and investigate complaints of wrongdoing. We have noted a range of existing mechanisms for receiving complaints but, as consultees broadly agreed, these mechanisms have been variously criticised for being insufficiently expeditious, insufficiently independent, and insufficiently equipped to conduct the necessary investigations. Our proposal for a statutory commissioner was generally supported by consultees (albeit that some were concerned that a statutory commissioner model that lacked the fortification afforded by a public interest defence would be insufficient).

8.126 Many consultees provided helpful feedback on our consultation questions relating to a public interest defence. In our Consultation Paper, we presented a number of concerns with such a defence. We were keen for feedback from consultees on the extent to which these concerns could be mitigated. The feedback that we received allowed us to reconsider the matter and was helpful in informing our final view which, combined with our detailed assessment of Article 10 ECHR in the following chapter, supports our recommendation in favour of a public interest defence.

8.127 Yet our recommendation for a statutory commissioner, fortified by a public interest defence, has a broader objective than compliance with Article 10. It is about a fair law that takes seriously the public interests in national security and in accountable Government. As we noted at the beginning of this chapter, national security should not come at the expense of the rule of law, just as the price of accountability should not be the proper, legal protection of the UK – its interest, its public servants, and its people.

8.128 The model that we recommend is designed to provide a fair and effective way of balancing these interests. It allows for disclosure sufficient to prompt meaningful investigation and, where appropriate, redress for wrongdoing. It allows for this disclosure without risking damage to the public interest (as is unavoidably a risk with unauthorised public disclosures, no matter the sincerity of the discloser). Finally, where the discloser chooses to make an unauthorised disclosure regardless of the existence of a body charged with considering these public interest complaints, it will

---

547 *R v Sarker* [2018] EWCA Crim 1341, [2014] 4 All ER 694 at [29].

be open to that person to argue at trial that the disclosure, taken as a whole and considering the manner of disclosure, was in the public interest.

8.129 We now turn, over the following chapters, to consider these recommendations in detail, as well as the UK's obligations under Article 10.

Chapter 9: Article 10 of the European Convention on Human Rights

INTRODUCTION

9.1 The purpose of this chapter is to consider the extent to which the offences in the Official Secrets Act 1989 ("OSA 1989") that criminalise the unauthorised disclosure of information are compatible with the right to freedom of expression. In our Consultation Paper, we provisionally concluded that the offences contained in the OSA 1989 are compatible with Article 10 of the European Convention on Human Rights ("ECHR") on the basis that they constitute a proportionate interference with the right to freedom of expression. We reached this provisional conclusion even though there is currently no public interest defence in the relevant legislation.

9.2 In this Report, and following feedback from consultees, we have taken this opportunity to review our position on Article 10. We consider the case law as it relates both to public servants and to journalists. The case law has demonstrated the importance that the European Court of Human Rights ("ECtHR" or "the Court") places upon the public servants' duty of loyalty, discretion and reserve. In the absence of a decision of the ECtHR expressly stating what protection should be afforded to journalists who breach domestic official secrecy laws, we consider whether compliance with Article 10 would require that a public interest defence be made available under the OSA 1989.

9.3 Further, we consider the House of Lords decision in *R v Shayler*,[548] which is currently binding law in the UK on the compatibility with Article 10 of the UK's official secrets regime (or parts thereof). Specifically, in response to a number of consultees' arguments, we consider whether the case would be decided differently in light of subsequent case law from the ECtHR.

9.4 Finally, we consider the responses to our consultation question as to whether a public interest defence is mandated by Article 10.

9.5 As a preliminary point, it is important to note that the Court's case law is not explicit enough to allow us to make conclusive determinations about whether the OSA 1989 is compatible with Article 10, nor (if it is not) what reforms would be certain to make it so. Such assessments cannot be made in a vacuum. The ECtHR will make a determination of Article 10 compliance on the specific facts of a given case, but will not rule that a regime is, and will be at all times, in compliance. The simple question for the Court in any case, in terms of Article 10, is whether sufficient protection was afforded to the applicant's freedom of expression. Of course, it is possible to make predictions about whether a given set of facts is likely to give rise to a valid claim under Article 10. By extension, it is possible to make predictions about the range of cases in which a regime is likely to be compliant. It is on this basis that we analyse the UK's protection of official data regime.

---

548 *R v Shayler* [2002] UKHL 11, [2003] 1 AC 247.

9.6 We conclude that we are unable to state with confidence that the current regime, even with its opportunities for Crown servants to report to the various bodies as discussed in Chapter 8 will, in all cases of unauthorised disclosure, afford adequate protection to Article 10 rights. Whilst there is a possibility that the binding domestic case, *Shayler*, would be decided the same way today *on its facts*, it is clear from the development of both domestic and European jurisprudence that a case founded on slightly different facts may well be decided differently and on different reasoning. There is, in any case, a real possibility that *Shayler* would be decided differently today.

9.7 As a result, we cannot rule out the possibility that a prosecution under the OSA 1989 as currently drafted, with no public interest defence available, would violate Article 10 ECHR in some cases, depending on the facts. For example, if the disclosure were made as a last resort, the prosecution was only for the purpose of protecting confidentiality in the information and not national security, and there was a serious public interest in disclosing the information, then it is likely that a prosecution under the OSA 1989 would be contrary to the ECHR and the Human Rights Act 1998.

9.8 We consider the need for a public interest defence at greater length in Chapter 11.

ARTICLE 10 – AN OVERVIEW

9.9 Article 10 of the European Convention on Human Rights (ECHR) provides that:

> (1) 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.
>
> (2) 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 reputations or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary.

9.10 The ECtHR has emphasised in a number of 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".[549]

9.11 Clayton and Tomlinson explain that the ECtHR assess the legality of an interference with Article 10 in the following way:

> 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 they delivered pursuant to their power of appreciation. This does not mean that the supervision is limited to ascertaining

[549] *Handyside v United Kingdom (5493/72)* [1976] ECHR 5, (1976) 1 EHRR 737 at [49].

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.[550]

9.12 Although Article 10 required Member States to be able to justify interference with freedom of expression, English law has long recognised the importance of freedom of expression, a freedom which "is subject only to clearly defined exceptions as laid down by common law and statute."[551] Indeed, as a number of consultees were right to note, the freedom accorded to the press to report instances of wrongdoing has ensured that the press have revealed many matters it was in the public interest to know.[552] We take seriously the public interest in the fundamental right to freedom of expression and do not underestimate the extent to which democracy rests on such a freedom.

WHAT DOES COMPLIANCE WITH ARTICLE 10 REQUIRE?

9.13 Whilst it is well recognised that freedom of expression is vital to the existence of democracy,[553] it is equally well recognised that this freedom is not unlimited: "the publication of information in the mass media can violate other rights and freedoms and have a clear and direct impact on the political process."[554] The right to freedom of expression is therefore not absolute (unlike, say, the right to life or the right not to be subject to torture), but is qualified. Balancing the competing freedoms and interests is not a simple binary exercise; on any given set of facts, increased compliance with one interest or Convention right may therefore come at the expense of another interest or Convention right. An obvious example, well known to the media and defamation lawyers, would be that allowing unfettered freedom of expression (ensuring maximum compliance with Article 10) would necessarily mean lesser compliance with Article 8 (the right to respect for private and family life). Whether a provision in domestic law complies with a qualified Convention right is therefore a question of degree. However, it is necessary to consider what might constitute the minimum protections that the UK should have in place to ensure that a prosecution involves no breach of Article 10. This question tends to be viewed in an alternative formulation: if we are interfering with the right, what is the minimum set of safeguards applicable so that the interference achieves compliance with Article 10?

---

550 R Clayton and H Tomlinson, *The Law of Human Rights* (2nd edn, OUP 2010) 15.239.

551 *R v Central Independence Television plc* [1994] Fam 192, 203 (Hoffman LJ).

552 The Guardian cited three examples at p2 of its consultation response: the UK's involvement in the running of a prison in Baghdad that was the scene of human rights abuses; collusion between police and loyalist terrorists; and the workings of a Metropolitan Police undercover unit.

553 See, for example, E Barendt, *Freedom of Speech* (Clarendon Press 1985).

554 R Clayton and H Tomlinson, *The Law of Human Rights* (OUP 2000) 15.04.

9.14 These questions are unavoidably context-dependent, and this will have a bearing on the confidence one can have in whether the current legislation that allows for prosecutions is compatible with Article 10. At a very general level, in order to comply with Article 10, any interference with the right to freedom of expression must satisfy the following criteria:

(1) the interference must be prescribed by law;

(2) the interference must seek to pursue one of the legitimate aims listed in Article 10(2); and

(3) the interference must be necessary in a democratic society.

Is the interference prescribed by law?

9.15 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.[555]

9.16 In *Sunday Times v United Kingdom,* it was held that for a law to be compliant with this aspect of the Convention right, the citizen must be able to foresee, if necessary with "appropriate advice", the legal consequence a given action may entail.[556]

9.17 In our Consultation Paper, we took the view that these criteria were satisfied by the Official Secrets Act 1989, given that the offences are contained in public legislation and are drafted with sufficient specificity. This proved to be uncontroversial.

Does the interference pursue a legitimate aim?

9.18 An interference with Article 10(1) will only be justified if it pursues one of the legitimate aims listed in Article 10(2) as set out above (national security, territorial integrity etc). 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.[557] They do suggest, however, that the legitimate aim relied upon will be relevant to the breadth of the "margin of appreciation" the ECtHR affords the State.[558] The margin of appreciation determines how far the Court will leave the practical application of Article 10 in specific cases to the national institutions of the state in question. It seems clear that the Court would provide a greater margin of appreciation to the State where the interest being protected was national security than a less important interest.

9.19 In our Consultation Paper, we explained that, in the context of unauthorised disclosure offences, there are two legitimate aims that are relevant: national security, and the

---

555 R Clayton and H Tomlinson, *The Law of Human Rights* (2nd edn, OUP 2010) 15.299.

556 *The Sunday Times v United Kingdom (6538/74)* [1979] ECHR 9, (1979) 2 EHRR 245 at [49].

557 R Clayton and H Tomlinson, *The Law of Human Rights* (2nd edn, OUP 2010) 15.305.

558 R Clayton and H Tomlinson, *The Law of Human Rights* (2nd edn, OUP 2010) 15.305.

protection of the reputation and rights of others. We also consider that preventing the disclosure of information received in confidence could be a legitimate aim. These are legitimate aims because the justification for the existence of the offences contained in the Official Secrets Act 1989 is the protection of information that falls into those categories: broadly speaking, national security, the prevention of crime, and preventing the disclosure of information received in confidence.[559]

Is the interference necessary in a democratic society?

9.20 The first two questions in 9.15 having been answered positively, it is still open to the Court to find that the interference prescribed by law "is greater than is required to meet the legitimate object which the state seeks to achieve."[560] The interference could be in bad faith or disproportionate, for example.

9.21 As we discussed in our Consultation Paper, the task of the ECtHR is to assess whether the interference complained of (ie the existence of the criminal offences contained in the Official Secrets Acts[561]) corresponds to a "pressing social need", whether it is proportionate to the legitimate aim pursued and whether the reasons given by the national authority to justify it are relevant and sufficient to justify the interference.[562]

9.22 This aspect of our analysis generated the greatest volume of responses from consultees. Those consultees who responded to this chapter of our Consultation Paper focused their responses on the issue of proportionality and, in particular, the continuing validity of the approach taken by the House of Lords in *R v Shayler* (the leading domestic authority on the compatibility of the Official Secrets Act 1989 with Article 10).[563] Therefore, it will be of benefit to consider the question of proportionality in detail.

9.23 It is clear from ECHR case law that "necessary" is synonymous neither with "indispensable" nor with merely "desirable" or "useful" (*Handyside v United Kingdom*[564]). As held by Lord Hope in *Shayler*, citing paragraph [49] of the court's judgment in *Handyside*, "the word 'necessary' in article 10(2) introduces the principle of proportionality."[565]

---

559 Prevention of crime seems the relevant objective for section 4(2) OSA 1989, and the protection of information received in confidence would be relevant to section 3.

560 *R v Shayler* [2002] UKHL 11, [2003] 1 AC 247 at [26] (Lord Bingham of Cornhill).

561 Though there is no Article 10 jurisprudence on this direct point, it is noteworthy that the ECtHR held, in *Dudgeon v United Kingdom* [1983] ECHR 2, (1983) 5 EHRR 573 at [41], that "the maintenance in force of the impugned legislation [prohibiting homosexual acts between consenting adult men] constitutes a continuing interference with the applicant's right…: [E]ither he respects the law and refrains from engaging… in prohibited sexual acts to which he is disposed by reason of his homosexual tendencies, or he commits such acts and thereby becomes liable to criminal prosecution."

562 *The Sunday Times v United Kingdom (6538/74)* [1979] ECHR 9, (1979) 2 EHRR 245 at [62].

563 *R v Shayler* [2002] UKHL 11, [2003] 1 AC 247.

564 *Handyside v United Kingdom (5493/72)* [1976] ECHR 5, (1976) 1 EHRR 737 at [48].

565 *R v Shayler* [2002] UKHL 11, [2003] 1 AC 247 at [57] (Lord Hope of Craighead).

9.24 The ECtHR has held that there are a number of factors that it may consider in determining proportionality.[566] In doing so, it will consider:

(1) the public interest in the disclosed information;

(2) the authenticity of the disclosed information;

(3) the damage suffered by the public authority as a result of the disclosure;

(4) the motive behind the disclosure;[567]

(5) the penalty imposed on the discloser and its consequences;[568] and

(6) whether there were alternative mechanisms by which the discloser could have sought to address their concerns, and whether public disclosure was made as a last resort.[569]

9.25 The considerations will not have equal weight in each case and, as will be seen below, the case law seems to suggest that (6) will hold particular significance in the court's determination of compliance in cases involving public servants. Even where the applicant's motive was noble,[570] and the subject matter both true and in the public interest (ie making clear government wrongdoing), the question of whether there existed effective alternative mechanisms seems broadly to be determinative.

9.26 There is long-standing ECHR case law (see, for example, *Klass v Germany*) supporting the view that states are entitled to take measures which enable them effectively to counter threats to national security, but that there must exist "adequate and effective guarantees against abuse" of these measures.[571] As the Court held in *Klass*, the assessment of adequacy and effectiveness "has only a relative character: it depends on all the circumstances of the case".[572]

9.27 Lord Sumption's consideration of the proportionality test in *Bank Mellat v Her Majesty's Treasury (No 2)* included an assessment of "whether, having regard to these matters and to the severity of the consequences, a fair balance has been struck between the rights of the individual and the interests of the community."[573] In that case, HM Treasury had taken measures to restrict Bank Mellat – an Iranian commercial bank – from operating within the United Kingdom's financial markets. They had done so in order to frustrate, as far as possible, Iran's weapons programme. However, comparable banks had not been subject to the same order, and broadly the same objective could have been achieved by requiring banks "to observe financial

---

566 *Guja v Moldova (14277/04)* [2008] ECHR 144, (2011) 53 EHRR 16.

567 *Guja v Moldova (14277/04)* [2008] ECHR 144, (2011) 53 EHRR 16 at [85]-[88].

568 *Guja v Moldova (14277/04)* [2008] ECHR 144, (2011) 53 EHRR 16 at [95]-[96].

569 *Guja v Moldova (14277/04)* [2008] ECHR 144, (2011) 53 EHRR 16 at [73].

570 Which is to say, neither motivated by malice nor grudge, nor by financial gain.

571 *Klass and others v Germany (5029/71)* [1978] ECHR 4, (1978) 2 EHRR 214 at [50].

572 *Klass and others v Germany (5029/71)* [1978] ECHR 4, (1978) 2 EHRR 214 at [50].

573 *Bank Mellat v Her Majesty's Treasury (No 2)* [2013] UKSC 39 at [20] (Lord Sumption).

sanctions and relevant risk warnings."[574] The risks attended to the banking sector generally, and not to Bank Mellat specifically. The interference was therefore disproportionate not only because it went beyond what was necessary to secure its objective, but also because there was no rational link between the uniquely detrimental effect on the defendant and on the objective sought.[575]

9.28 Therefore, as Lord Hope identified in his speech in *Shayler,* states cannot assume that merely demonstrating "in general terms that a restriction on disclosure is needed in the interests of national security" will ensure compliance with Article 10.[576] Any assertion that an interference in the fundamental right to freedom of expression is proportionate must therefore pay due heed to the facts of the case in question.

9.29 For the avoidance of doubt, then, there is a balance to be struck between competing legitimate interests. The balance will not be struck by a blanket criminalisation of unauthorised disclosures. However, nor will it be struck by granting a licence to disclose material to whomever one pleases. The public interest will be likely to be served best by a form of disclosure that allows for effective remedy and redress of the subject-matter of the whistleblowing, for example, whilst posing the least possible threat to Convention rights and national security.

9.30 There are, however, different considerations with respect to (a) public servants who owe a duty of loyalty and confidence to the government, and (b) to journalists. The question of what constitutes a proportionate interference will receive a different answer with respect to each category of person. It is worth, therefore, considering each in turn.

ARTICLE 10 AND PUBLIC SERVANTS

9.31 It is clear from European human rights case law since *Shayler* that the fundamental approach to proportionality described above has not changed, albeit that the consideration of the proportionality question has become more sophisticated.

Duty of discretion

9.32 In the context of disclosures by public servants, the ECtHR's starting point is that Article 10 applies in the workplace and employees, including public servants, enjoy the right to freedom of expression.[577] However, at the same time, public servants owe particularly strong duties of "loyalty, reserve, and discretion"[578] to their employers.

9.33 Hence, in *Hadjianastassiou v Greece* it was held that there had been no violation of Article 10 when an officer in the Greek Air Force was found guilty of disclosing military secrets without authorisation. The ECtHR stated that:

---

574 *Bank Mellat v Her Majesty's Treasury (No 2)* [2013] UKSC 39 at [27] (Lord Sumption).

575 *Bank Mellat v Her Majesty's Treasury (No 2)* [2013] UKSC 39 at [27] (Lord Sumption).

576 *R v Shayler* [2002] UKHL 11, [2003] 1 AC 247 at [68] (Lord Hope of Craighead).

577 See for example *Guja v Moldova (14277/04)* [2008] ECHR 144, (2011) 53 EHRR 16 at [70].

578 *Guja v Moldova (14277/04)* [2008] ECHR 144, (2011) 53 EHRR 16 at [70].

> It is also necessary to take into account the special conditions attaching to military life and the specific "duties" and "responsibilities" incumbent on members of the armed forces. The applicant, as the officer at the KETA [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.[579]

9.34 The judgment in *Guja v Moldova* demonstrates how wide a margin of appreciation the Court will grant to states when it comes to the interference with the Article 10 rights of public servants. In *Guja*, the Court held that the interference in Article 10 was disproportionate because, on the facts, the applicant had no further, effective means of remedying the governmental wrongdoing. The applicant had disclosed evidence of corruption to a newspaper. There were various theoretical avenues for redress open to the applicant (such as reporting the alleged corruption to the Prosecutor General's Office); had these been effective, it seems very likely that the Court would have found in favour of Moldova. However, the Court was persuaded that, in practice, the applicant had no other effective means of remedying the relevant governmental wrongdoing apart from making an external report. Thus, disclosure to the newspaper was the last and only resort.[580] The Court stated that:

> Since the mission of civil servants in a democratic society is to assist the government in discharging its functions and since the public has a right to expect that they will help and not hinder the democratically elected government, the duty of loyalty and reserve assumes special significance for them … In addition, in view of the very nature of their position, civil servants often have access to information which the government, for various legitimate reasons, may have an interest in keeping confidential or secret. Therefore, the duty of discretion owed by civil servants will also generally be a strong one.[581]

9.35 This is so even though *Guja* did not concern national security directly; the legitimate aim of the legislation was to prevent the disclosure of information received in confidence. Given the obligation of the Court to examine whether there was a proportionate relationship between the interference and the aim thereby pursued, it is certainly arguable that the margin of appreciation might be wider where the aim is national security rather than a breach of confidence. Nonetheless, *Guja* has been applied in notable cases concerning national security (such as those considered here).

9.36 More recently, the Court in *Catalan v Romania*[582] stated that the term "duties and responsibilities" in Article 10(2) has a special meaning in respect of public servants, which justifies leaving to the state a wider margin of appreciation. Disclosures that

---

579 *Hadjianastassiou v Greece (12945/87)* [1992] ECHR 78, (1993) 16 EHRR 219 at [46].

580 *Guja v Moldova (14277/04)* [2008] ECHR 144, (2011) 53 EHRR 16 at [81]-[84].

581 *Guja v Moldova (14277/04)* [2008] ECHR 144, (2011) 53 EHRR 16 at [71].

582 *Catalan v Romania (13003/04)* [2018] ECHR 6. The case concerned the dismissal of a civil servant (Mr Catalan). C was in the employ of the National Council for the Study of *Securitate* Archives (CNSAS). The CNSAS had a role in informing the public about historic collaboration with the *Securitate* (the former political police under the communist regime). C disclosed information to the press claiming that a religious leader had collaborated with the *Securitate*, and did so without authorisation from his employer. The domestic court, confirming his dismissal, found that he had breached his duty of discretion as a civil servant.

might be legitimate in other contexts are not necessarily legitimate in these employment relationships.[583]

9.37 Of particular interest in *Catalan* was the Court's finding that the behaviour of the applicant – the public servant who was prosecuted for the leak - was intended "à alimenter la presse dite « de divertissement »" – to feed the 'entertainment' press – and risked distorting public opinion by presenting his remarks as certainties. This was not, therefore, a disclosure in the spirit of serious academic inquiry.[584] Even if there were some public interest in the disclosure, the duty of reserve owed to the employer was not completely erased by that public interest.[585] Thus, in assessing the extent to which the duty owed to the employer could be avoided, it was necessary to consider the fact that the disclosure had risked manipulating public opinion (even more so because the employer in this case – the National Council for the Study of Securitate Archives – was tasked with the provision of reliable and trustworthy information).[586]

Effective means of remedying the wrongdoing

9.38 In light of this duty of discretion on the part of public servants, the court in *Guja* held that "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".[587] Therefore, "[i]n assessing whether the restriction on freedom of expression was proportionate… 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."[588] This formulation has been cited with approval in subsequent case law: in particular, *Heinisch v Germany*[589] and *Bucur and Toma v Romania.*[590]

9.39 In *Heinisch v Germany,* Ms Heinisch had made a number of complaints to her superiors. No investigation or redress was forthcoming, and thus the applicant made a formal criminal complaint against her employer. The Court was of the opinion that the duty of loyalty had been complied with in drawing the factual bases of the criminal complaint to the employer's attention, and that their failure to investigate or remedy unlawful practice meant that the applicant was no longer bound by the duty of loyalty.[591] The lack of effective investigative or enforcement mechanism meant that external disclosure by means of a criminal complaint was justifiable.[592]

---

583 *Catalan v Romania (13003/04)* [2018] ECHR 6 at [57]-[58].

584 *Catalan v Romania (13003/04)* [2018] ECHR 6 at [67]-[68].

585 *Catalan v Romania (13003/04)* [2018] ECHR 6 at [69].

586 *Catalan v Romania (13003/04)* [2018] ECHR 6 at [69].

587 *Guja v Moldova (14277/04)* [2008] ECHR 144, (2011) 53 EHRR 16 at [73].

588 *Guja v Moldova (14277/04)* [2008] ECHR 144, (2011) 53 EHRR 16 at [73].

589 *Heinisch v Germany (28274/08)* [2011] ECHR 1175, (2014) 58 EHRR 31 at [65].

590 *Bucur and Toma v Romania (40238/02)* [2013] ECHR 14 at [93].

591 *Heinisch v Germany (28274/08)* [2011] ECHR 1175, (2014) 58 EHRR 31 at [73]-[74].

592 *Heinisch v Germany (28274/08)* [2011] ECHR 1175, (2014) 58 EHRR 31 at [75]-[76].

9.40 In *Bucur and Toma*, the Court was of the view that protection should be afforded to employees who disclose information via 'external' channels where it is clear that the internal channels (if they even exist) either do not work properly or where it would be unreasonable to expect them to work properly given the nature of the information disclosed by the employee.[593]

9.41 In *Guja* (facts at 9.34 above), the Court was persuaded by the following factors:

(1) there was no prescribed procedure for the reporting of irregularities by employees to the Prosecutor General's Office; and

(2) the Prosecutor General's Office was not meaningfully independent of the subject of the complaint.[594]

9.42 This second limb is, of course, a fundamental aspect of "effectiveness". A body is not likely to be sufficiently independent if they are themselves the subject of the complaint. In *Bucur and Toma* the only available internal channel for redress was for the applicant to report to his superiors, but the alleged irregularities concerned his superiors directly; in those circumstances, the Court doubted the effectiveness of any report the applicant could have made to his superiors.[595]

9.43 In *Guja*, the Prosecutor General was not the subject of the complaint. However, he had been aware of the wrongdoing for around six months and had manifested no intention to respond, having "succumbed to the pressure that had been imposed on his office".[596] Hence, it was clear that the Prosecutor General's Office lacked meaningful independence.

9.44 We consider in the following chapter how this jurisprudence from Strasbourg has informed our conclusions on the attributes that an investigative mechanism must have in order to be effective. Our conclusion, based on the above, is that where an effective investigative mechanism existed, but where the public servant chose not to use it, the ECtHR would not be likely to find a breach of Article 10.

HOW WOULD *SHAYLER* BE DECIDED TODAY?

9.45 A number of consultees suggested that, given the development of ECHR case law in relation to public servants, the UK Supreme Court would not follow the House of Lords' decision in *R v Shayler* were it to be asked to rule on the same substantive issues today.[597] We considered that it was important to devote a significant portion of the chapter in our Consultation Paper to this judgment as it remains binding as a matter of domestic law. It is also the only domestic case to have considered this issue directly. Since consultees focused a significant amount of attention on *Shayler* too, it is necessary to consider the judgment in detail again in this Report.

---

593 *Bucur and Toma v Romania (40238/02)* [2013] ECHR 14 at [97].

594 *Guja v Moldova (14277/04)* [2008] ECHR 144, (2011) 53 EHRR 16 at [81]-[84].

595 *Bucur and Toma v Romania (40238/02)* [2013] ECHR 14 at [97].

596 *Guja v Moldova (14277/04)* [2008] ECHR 144, (2011) 53 EHRR 16 at [82].

597 *R v Shayler* [2002] UKHL 11, [2003] 1 AC 247.

Summary of the judgment

9.46 The question before the House of Lords was whether the prosecution under sections 1(1)(a), 4(1) and 4(3) of the Official Secrets Act 1989 was compatible with Article 10 of the ECHR. The defendant was a former member of the Security Service who disclosed to a newspaper information which had been obtained in the course of his employment. He had not attempted to make use of any internal (ie authorised) complaints or disclosure mechanisms. He was charged with offences contrary to sections 1(1)(a), 4(1) and 4(3) of the Act. A preliminary question arose as to whether compatibility with Article 10 ECHR required the defendant to be afforded a defence if, as submitted on his behalf, it was found that the disclosure was in the public interest.

The need to preserve confidentiality

9.47 In rejecting this argument in the House of Lords, Lord Bingham of Cornhill 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.[598]

9.48 Lord Bingham also cited a number of domestic authorities pointing to the need for the security and intelligence services to work in secret.[599] In support of this proposition, the following passage of Lord Griffiths in *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 bright line 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.[600]

9.49 Lord Hope held that the regime established by the Official Secrets Act 1989 came

---

598 *R v Shayler* [2002] UKHL 11, [2003] 1 AC 247 at [26].

599 *R v Shayler* [2002] UKHL 11, [2003] 1 AC 247 at [25].

600 *R v Shayler* [2002] UKHL 11, [2003] 1 AC 247 at [25] citing *Attorney General v Guardian Newspaper (No 2)* [1990] 1 AC 269 (Lord Griffiths).

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.[601]

9.50 It was held that a system requiring explicit 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.[602]

9.51 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.[603]

Channels for authorised disclosure

9.52 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.[604] Rather, as he stated, the Official Secrets Act 1989 imposes a prohibition on disclosure *without lawful authority*. Lord Bingham then proceeded to set out those office holders to whom a former member of the security and intelligence agencies could make a lawful disclosure:

(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".[605]

(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

---

601 *R v Shayler* [2002] UKHL 11, [2003] 1 AC 247 at [80].

602 *R v Shayler* [2002] UKHL 11, [2003] 1 AC 247 at [84].

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

604 *R v Shayler* [2002] UKHL 11, [2003] 1 AC 247 at [27].

605 *R v Shayler* [2002] UKHL 11, [2003] 1 AC 247 at [27].

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, 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 Controller and Auditor General, the National Audit Office and the Parliamentary Commissioner for Administration.[606]

9.53 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.[607]

9.54 By contrast, Lord Hope expressed some unease with certain aspects of the Official Secrets Act 1989.[608] Though 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,[609] he was nonetheless concerned about the effectiveness of these options in curbing abuses in all cases:

> 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 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.[610]

---

606 *R v Shayler* [2002] UKHL 11, [2003] 1 AC 247 at [27].

607 *R v Shayler* [2002] UKHL 11, [2003] 1 AC 247 at [29].

608 *R v Shayler* [2002] UKHL 11, [2003] 1 AC 247 at [40]-[41].

609 *R v Shayler* [2002] UKHL 11, [2003] 1 AC 247 at [63].

610 *R v Shayler* [2002] UKHL 11, [2003] 1 AC 247 at [70].

9.55 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.[611]

9.56 However, he also noted that Shayler's decision not to seek authorisation rendered his concerns somewhat theoretical as far as the case was concerned. The fact that in this case Shayler 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.[612]

Judicial review of unjust refusal of authorisation

9.57 Although Lord Bingham expected that official authorisation would only be withheld when an adequate justification existed, he did recognise the possibility that authorisation could be withheld despite the fact no such justification existed. In such circumstances, the individual in question could seek judicial review of a decision to refuse authorisation. As the decision to refuse authorisation impacts upon a right enshrined in the ECHR, Lord Bingham stated that any such refusal must be subject to rigorous scrutiny. Given that this would be the case, Lord Bingham held that judicial review offered sufficient protection for individuals in the appellant's position.[613]

9.58 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.[614]

9.59 Lord Bingham also considered the argument that judicial review was an illusory option in terms of the protection it offered to a member or former member of the service, because the applicant would be unable to instruct a lawyer of his choosing without committing further offences (on this point, see also Chapter 6:). In rejecting this argument, Lord Bingham stated:

---

611 *R v Shayler* [2002] UKHL 11, [2003] 1 AC 247 at [71].

612 *R v Shayler* [2002] UKHL 11, [2003] 1 AC 247 at [70].

613 *R v Shayler* [2002] UKHL 11, [2003] 1 AC 247 at [32]-[34].

614 *R v Shayler* [2002] UKHL 11, [2003] 1 AC 247 at [33].

> 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.[615]

9.60 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 compliance with the requirements of Article 10(2).[616]

Attorney General consent

9.61 Lord Bingham also cited (at [35]) the requirement for the Attorney General's 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 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.[617]

Concluding remarks

9.62 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*

---

615 *R v Shayler* [2002] UKHL 11, [2003] 1 AC 247 at [34]. So stated, this is not the position that we adopt (see the discussion in Chapter 5), though we recommend that there should be circumstances in which disclosures to legal advisers would be authorised disclosures (and so not offences). We agree with Lord Bingham to the extent that it should never be the case that the former member is unable to seek legal advice.

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

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

part, from that undertaking he must seek authorisation and, if so advised, challenge any refusal of authorisation.[618]

9.63 Lord Hobhouse, Lord Hutton and Lord Scott agreed with the judgment of Lord Bingham.

How would the case be decided today?

9.64 We share the view of some consultees that the consideration of the proportionality of prosecution for unauthorised disclosure will differ in substance (if not always outcome) in UK judgments that may be handed down in the future. Our analysis of the ECHR case law led us to conclude that it is necessary to ensure that an effective mechanism exists to investigate Crown servants' concerns. We do not consider that the current range of options available to a Crown servant is adequate to ensure compliance with Article 10. Foremost in this assessment is the fact that none of the options is independent of government or of the police, security and intelligence services. The lack of independence would weigh in favour of an argument that public disclosure was a last resort. We must acknowledge, therefore, a real possibility that a case similar to *Shayler* would be decided differently today.

9.65 There is a good argument, of course, that *Shayler* might be decided the same way on its very specific facts (albeit that the reasoning would be different): it is noteworthy, for example, that Shayler was in contact with journalists without making use of official channels. The fact that Shayler did not attempt to use any reporting mechanism meant that no meaningful judgment could be reached as to the effectiveness of those mechanisms that did exist. Although their Lordships expressed appropriate caution in considering whether these mechanisms would be sufficient in every conceivable case, the fact remains that Shayler could not convincingly state that there was no effective mechanism available to him. This was a failing emphasised by their Lordships in *Shayler*.[619]

9.66 Further, the failure to use the mechanisms available may import questions of bad faith. As with *Catalan*, a defendant's deliberate failure to use the reporting channels available to him or her without good reason may lead to the conclusion that direct disclosure to the press was not simply a search for redress.

9.67 However, it would be going too far to suggest that a defendant would actually have to attempt to use the reporting mechanisms in order to demonstrate that they were ineffective; there are clearly instances where such ineffectiveness would be obvious to the objective observer before the fact (recall, for example, *Bucur and Toma v Romania* in which it was clear that a report could not be made to the applicants' superiors given that the report concerned their superiors[620]). It is possible Shayler could have pointed to the lack of independence as proof that the mechanisms would have been ineffective. (We concede, of course, that this would require more than theoretical disparagement: the ECtHR, following *Guja* and subsequent case law,[621]

---

618 *R v Shayler* [2002] UKHL 11, [2003] 1 AC 247 at [36] (emphasis added).

619 *R v Shayler* [2002] UKHL 11, [2003] 1 AC 247 at [36].

620 *Bucur and Toma v Romania (40238/02)* [2013] ECHR 14.

621 As discussed at length above.

would have to be reasonably convinced that public disclosure was the last resort and therefore protected by Article 10).

9.68 Further, a case based on slightly different facts may well not be decided in the same way. For example, where the protected information is merely confidential and not related to national security or crime and the public interest in disclosure is strong, the lack of availability of a public interest defence may generate more searching questions about whether the scheme is compatible with Art 10. Even in those situations, however, the availability of effective investigative mechanisms would inevitably weigh in the balance, on the basis of current case law.

9.69 Recalling Lord Sumption's judgment in *Bank Mellat*, in future cases, even when a legitimate aim is being pursued and with no more interference than necessary, it will be important to consider in detail how the interference operates and especially whether the effect on the individual can be justified having in mind the interests of the community.[622] The assessment is intensely fact-dependant, and will necessarily include a variety of considerations, including:

(1) the sensitivity of the information disclosed;

(2) whether an effective investigative mechanism was available (and effectiveness imports independence);

(3) whether the Crown servant tried to use those mechanisms; and

(4) whether the Crown was acting in good faith.

9.70 By way of summary conclusion of this section, we conclude that, while there is an argument that *Shayler* is correct on its facts, there is a real possibility that it would be decided differently today on not wholly dissimilar facts. We cannot be confident that, in other cases, to follow *Shayler* would be to respect Article 10. A worst-case scenario, as an example of this point, would be a case where a Crown servant made an unauthorised disclosure in good faith because, despite some internal mechanism being available to him or her, that mechanism either failed (perhaps, say, due to the urgency of the matter) or there was good reason not to use it.

ARTICLE 10 AND THE MEDIA

9.71 As consultees emphasised, it is necessary to consider the extent to which any provision which has the potential to impact upon journalistic activity is compatible with Article 10. We accept the point made by Guardian News and Media and News UK, amongst others, that the Article 10 implications of prosecuting journalists require separate consideration. The discussion in this section is on the narrow issue of how the ECtHR assesses the proportionality of interferences in the freedom of expression of those engaged in journalistic activity. In particular, the discussion is concerned with the interference made by section 5 of the Official Secrets Act 1989. Section 5 provides:

---

622 *Bank Mellat v Her Majesty's Treasury (No 2)* [2013] UKSC 39 at [27] (Lord Sumption).

(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 her 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 her 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.

9.72 The primary reason that it is worth affording separate consideration to the matter of journalists is because the reasoning which was so fundamental to the ECtHR's conclusions on many of the decisions above would not apply directly to journalists. As we have seen, the ECtHR has considered the scope of protections for unauthorised disclosures by civil servants, but it is difficult to determine how the logic in such cases would apply to journalists. In *Guja v Moldova*, the ECtHR highlighted the "duty of loyalty, reserve and discretion" of employees generally, a duty that was "particularly so in the case of civil servants".[623] The Court recognised that there might be a "strong public interest" in the disclosure of information concerning:

> illegal conduct or wrongdoing… [where]… the employee or civil servant concerned is the only person, or part of a small category of persons, aware of what is happening at work and is thus best placed to act in the public interest by alerting the employer or the public at large.[624]

9.73 As we have discussed, the Court stated that disclosure to the public could only be as a "last resort" and where disclosure to a "superior or other competent authority or body" was "impracticable".[625]

9.74 Journalists do not owe the same duties of "loyalty, reserve and discretion" as civil servants, so the ECtHR's reference in *Guja v Moldova* to a public disclosure being a "last resort" is unlikely to apply in such a strict sense. Of course, just as with public servants, journalists may well have other avenues available to them to report concerns other than immediate public disclosure, and there is no reason to suppose (given the current case law) that the ECtHR would not take this into account in determining the proportionality of the interference. However, the lack of prior

---

623 *Guja v Moldova (14277/04)* [2008] ECHR 144, (2011) 53 EHRR 16 at [70].

624 *Guja v Moldova (14277/04)* [2008] ECHR 144, (2011) 53 EHRR 16 at [72].

625 *Guja v Moldova (14277/04)* [2008] ECHR 144, (2011) 53 EHRR 16 at [73].

obligation on the journalist's part would suggest that "last resort" should be interpreted rather more broadly, affording the journalist's Article 10 rights greater latitude.

9.75 Further, the intensity of review of restrictions on freedom of expression and the margin of appreciation afforded to the state varies depending on the type of speech at issue and the nature of the legitimate interest that is invoked to justify restricting it.

9.76 The first point to note in considering this issue is that the type of speech is crucial. Political speech generally attracts more intensive review. This means that it is more difficult to justify restrictions on this type of speech. In *Wingrove v UK,* the ECtHR held that "there is little scope under Article 10(2) … for restrictions on political speech or on debate of questions of public interest" and contrasted this with the "sphere of morals" (for example, offending religious convictions), where a wider margin of appreciation is applied.[626]

9.77 Professor Feldman notes that restriction of speech, particularly by the media, which "may advance democratic participation or accountability",[627] is closely scrutinised by the ECtHR.

9.78 As consultees pointed out to us, and as noted by Professor Feldman, the ECtHR has stated that "freedom of expression constitutes one of the essential foundations of a democratic society and that the safeguards to be afforded to the press are of particular importance".[628] This point has been reiterated on numerous occasions by the ECtHR. For example, in *Bladet Tromsø and Stensaas v Norway*, the ECtHR stated that:

> The most careful scrutiny on the part of the Court is called for when, as in the present case, the measures taken or sanctions imposed by the national authority are capable of discouraging the participation of the press in debates over matters of legitimate public concern.[629]

9.79 The ECtHR has, on many previous occasions, recalled the need for "strict" or "careful scrutiny" of restrictions imposed on journalistic free expression.[630] This point was emphasised most recently by the ECtHR in *Big Brother Watch and others v UK.* In this case, the ECtHR stated that:

> The Court reiterates that freedom of expression constitutes one of the essential foundations of a democratic society and that the safeguards to be afforded to the press are of particular importance.[631]

---

626 *Wingrove v United Kingdom (17419/90)* [1996] ECHR 60, (1997) 24 EHRR 1 at [4d].

627 D Feldman (2002) *Civil Liberties and Human Rights in England and Wales.*

628 *Goodwin v the United Kingdom (17488/90)* [1996] ECHR 16, 22 EHRR 123; *Jersild v Denmark (15890/89)* [1994] ECHR 33, (1994) 19 EHRR 1.

629 *Bladet Tromsø and Stensaas v Norway* [1999] ECHR 29, (2000) 29 EHRR 125 at [64].

630 See, for example, *Independent News and Media and Independent Newspapers Ireland Limited v Ireland (55120/00)* [2005] ECHR 402, (2006) 42 EHRR 1024 at [114].

631 *Big Brother Watch and others v United Kingdom (58170/13)* [2018] ECHR 722.

9.80 The ECtHR has also held in numerous cases that restrictions on the ability of the press to *gather* and impart information of public interest require especially careful scrutiny.[632] Although the Court has stopped short of confirming a general right to receive information,[633] it is clear that the Court will interpret such a freedom as broadly as possible.[634] This is all the more so where barriers to information "exist solely because of an information monopoly held by the authorities."[635]

9.81 For the avoidance of doubt, however, this is not to be read as a positive obligation on the State's part to provide information. Following an extensive analysis of Article 10, Lord Mance in *Kennedy v The Charity Commission*[636] rejected the submission that Article 10 jurisprudence in Strasbourg supported – or was moving in the direction of – such an interpretation of the freedom of expression. Article 10 is not, to this extent, about transparent government. It restricts the manner in which states can interfere in freedom of expression, but the Strasbourg court has made clear on repeated occasions that Article 10 "does not give positive rights to require, or positive obligations to make, disclosure of information."[637]

9.82 The second point that is necessary to consider is the legitimate interest relied upon to justify the interference with the right. As we discuss above, the margin of appreciation afforded to the State may be wider where national security is at stake and narrower when some other legitimate interest is relied upon. Professors Fenwick and Phillipson note that, where proportionality needs to be assessed in the context of intelligence information and involves "a question of public judgment which courts are arguably ill-equipped to make", the margin of appreciation will generally be wider.[638] Therefore, a wider margin of appreciation might be expected in relation to security and defence information, which is encompassed by sections 1 and 2 of the Official Secrets Act 1989. The same wide margin of appreciation might be afforded in the context of territorial integrity or public safety (under the scope of would fall, for example, the offence under section 4 of the OSA 1989, which covers crime and investigation).

9.83 It seems less likely, therefore, that a violation of Article 10 would be found in the case of information relating to security, intelligence and defence. However, this is not to say that a case would always result in a particular outcome. In *Vereniging Weekblad Bluf! v Netherlands*, the ECtHR held that the seizure of publications disclosing the contents of an internal security service report was disproportionate because the historical nature of the information and previous wide publication meant that it was no longer necessary to protect it.[639] Professor Mowbray notes that this case:

---

632 See *Guseva v Bulgaria 6987/07* [2015] ECHR 171 at [53].

633 *Leander v Sweden 9248/81* [1987] ECHR 4, (1987) 9 EHRR 433.

634 *Sdružení Jihočeské Matky c. la République tchèque* [2006] ECHR 1205.

635 *Társaság a Szabadságjogokért v Hungary* [2009] ECHR 618, (2011) 53 EHRR 3 at [36].

636 *Kennedy v The Charity Commission* [2014] UKSC 20 at [57] – [89].

637 *Kennedy v The Charity Commission* [2014] UKSC 20 at [67] (Lord Mance).

638 H Fenwick and G Phillipson, *Media Freedom under the Human Rights Act* (2006) p 941.

639 *Vereniging Weekblad Bluf! v The Netherlands (16616/90)* [1995] ECHR 3, (1995) 20 EHRR 189.

reveals the Court making its own assessment of whether national security interests, even in the sensitive field of security service operations, require the limitation of freedom of expression concerning such activities.[640]

9.84 This suggests that the ECtHR may strictly scrutinise the prohibition of disclosures relating to security or intelligence where the proportionality analysis does not require difficult assessments or particular expertise. As the judgment in *Big Brother Watch and others v UK* demonstrates, there are instances of the ECtHR finding a violation of Article 10 even in the national security context.[641]

The offences applicable to journalists

9.85 It is worth recalling which OSA 1989 offences apply to journalists and might therefore constitute an interference in their Article 10 rights. The restrictions and penalties imposed by sections 5 and 6 of the OSA1989 are prescribed by law. Some, but not all, of the scenarios that could be prosecuted under these offences would be in the interests of national security, territorial integrity or public safety. This would apply to information disclosed contrary to section 1 or 2 of the OSA 1989. Some, but not all, information will be in the interests of the prevention of disorder or crime, such as information disclosed in contravention of section 4 of the OSA 1989. All the offences contained in the OSA 1989 criminalise the unauthorised disclosure of information received in confidence, either by preventing further dissemination following a breach of confidence or because the information was entrusted to the individual in confidence. The remainder of the disclosures prohibited by the OSA 1989, including some information relating to international relations disclosed contrary to section 3 of the OSA 1989, are only restricted in the interests of preventing disclosure received in confidence.

9.86 The issue that needs to be considered is under what circumstances the offences in sections 5 and 6 of the OSA 1989, and prosecution of those offences, might be "necessary in a democratic society" in the absence of a public interest defence. This question has never been considered by a domestic court or by the ECtHR, so we are attempting to answer it based upon the general principles expressed by the ECtHR.

Applying the ECtHR case law to the sections 5 and 6 offences

9.87 We repeat for emphasis the important point that not all disclosures encompassed by sections 5 and 6 of the OSA 1989 relate to national security, territorial integrity or public safety. Those relating to the prevention of crime encompass a large range of circumstances. This is a significant factor, since prohibiting disclosures in order to protect the integrity of investigations into serious crime will weigh more heavily in favour of proportionality than would be the case for disclosures which undermine investigations into minor crimes (albeit there is still a strong proportionality argument here). Similarly, the damage caused to international relations will range in severity, from the serious to the relatively trivial. The prohibition on disclosures which it is

---

640 A Mowbray, *Cases, Materials, and Commentary on the European Convention on Human Rights* (2012) p 710.

641 See *Big Brother Watch and others v United Kingdom (58170/13)* [2018] ECHR 722.

argued are in the public interest may therefore be disproportionate. It is not clear where such lines would be drawn by the ECtHR.

9.88 It is also necessary to bear in mind that the offences in sections 5 and 6 of the Official Secrets Act 1989 encompass a broad range of information. For example, a journalist who publishes material which advances democratic accountability in relation to a question of public interest, such as serious wrongdoing by a public official, might claim that the public interest in that being known outweighed the interest in maintaining confidentiality in the context of international relations, even where some limited damage is done. In a case such as this, if a prosecution were to be brought on the basis that an unauthorised disclosure of information related to international relations and the only damage proven was endangerment to the interests of the UK abroad in a cultural programme, such as the Olympics, rather than anything related to national security, we consider that the only legitimate aim that could be advanced for the purposes of Article 10(2) would be the protection of information received in confidence. The public interest in protecting such a programme could be outweighed by the public interest in disclosures related to serious wrongdoing, such as corruption.

9.89 If disclosure were a last resort, for example because internal mechanisms for investigating alleged wrongdoing were inadequate, then it is also possible that a prosecution would be held to constitute a disproportionate interference with Article 10 (as with non-journalistic activity, discussed earlier in this chapter). Prof Jacob Rowbottom also makes this submission in his response (see paragraph 9.123 below). Similarly, a disclosure relating to a matter of weighty public interest might outweigh any impact that disclosure had on the prevention of minor criminal offences. For example, where the revelation of major corruption resulted in the compromise of investigations into less serious crimes. In these cases, a public disclosure may well be afforded protection under Article 10.

9.90 It is worth noting that Article 10 has not been authoritatively interpreted, by the ECtHR, to require a public interest defence for journalists who are prosecuted for offences under official secrecy legislation. In Chapter 11, we consider the public interest defence in detail. For now, it suffices to conclude that, on the basis of existing ECHR case law, it is a real possibility that the ECtHR would hold that certain public disclosures by journalists would warrant protection by a specific statutory defence to offences under the 1989 Act. This would be especially so where the public interest in disclosure was found to be significant and the information did not relate to security, intelligence, defence or the prevention of serious crime. It is also a real possibility that the ECtHR would require a public interest defence for journalists where official and authorised means of reporting concerns about official wrongdoing are inadequate.

Consultation responses

9.91 The paucity of case law dealing with the interaction of Article 10 and sections 5 and 6 of the Official Secrets Act was reflected in the relevant consultation responses. News UK argued in their consultation response that *Shayler* was "not authority for the proposition that compliance with Article 10 does not require a public interest defence for *all* offences contained in the Official Secrets Act 1989". Rather, News UK argued, this case was only concerned with sections 1 and 4 of the Official Secrets Act 1989. They noted that the House of Lords in this case did not consider the offence contained

in section 5 of the Official Secrets Act 1989, which News UK pointed out is the offence that is "most likely to affect the media's work".

9.92 As far as News UK were concerned, there had not yet been a case which has considered whether the offence in section 5 of the Official Secrets Act 1989 is compatible with the ECtHR. It was argued that a media organisation, unlike the defendant in *Shayler*, could not "reasonably be expected to seek and obtain '*official authorisation*' before publishing in the same way as may be expected of a government employee".

9.93 News Group Newspapers submitted that *Shayler* would therefore not apply to a case where the prosecution was of a media organisation, who "cannot reasonably be expected" to seek official authorisation to disclose. (We are not sure how this submission squares with the Defence and Security Media Advisory Notice system). In their joint submission, English PEN, Index on Censorship and Reporters Without Borders shared this view, noting that:

> it is only in respect of the 'strict liability' offences under sections 1(1)(a) and 4(1) of the Official Secrets Act 1989 (unlawful disclosure by a member of the security or intelligence services and by a Crown servant or government contractor, respectively) that the House of Lords, in R v Shayler, confirmed that there is no public interest defence available, leaving it an open question whether such a defence might be available in respect of other offences under the Act.

9.94 The Guardian questioned whether the law as currently drafted would withstand a challenge based on restriction of access to information. In *Társaság a Szabadságjogokért v Hungary*[642] the ECtHR held that:

> In view of the interests protected by Article 10, the law cannot allow arbitrary restrictions which may become a form of indirect censorship should the authorities create obstacles to the gathering of information. For example, the latter activity is an essential preparatory step in journalism and is an inherent, protected part of press freedom.

9.95 The Guardian also argued that:

> The ECtHR recognised the public's right to receive information and the right of access to information via the media in cases such as *Leander v. Sweden*:[643] Article 10 "prohibits a government from restricting a person from receiving information that others wish or may be willing to impart to him". Similarly, in *Youth Initiative v Serbia,* 2013: "the gathering of information is an essential preparatory step in journalism and is an inherent, protected part of press freedom" and *Guseva v Bulgaria*, in 2015.[644] Thus, the hindering of access to information which is of public interest "may discourage those working in the media, or related fields, from pursuing such matters". As a result, they may no longer be able to play their vital role as "public

---

642 (2009) 53 EHRR 130 at [27].

643 Judgment of 26 March 1987, Series A No. 116.

644 See also *Shapovalov v Ukraine (45835/05)* [2012] ECHR 1665 at [68] and *Dammann v Switzerland (77551/01)* at [37].

watchdogs" and their ability to provide accurate and reliable information may be "adversely affected".

9.96 However, the Guardian did not indicate whether in its view, in the absence of a public interest defence, the Official Secrets Act 1989 would amount to an arbitrary restriction of the media to gather information and play their essential role in a democratic society. The Guardian concluded that "[j]ust as the very fact of a criminal conviction can have a disproportionate effect on journalistic expression, so can the use of criminal enforcement powers" and "[d]espite [the] lack of clear public appetite to prosecute journalists, the Law Commission's proposals are so broad – catching legitimate investigative journalistic practices – that the threat of imprisonment would unacceptably restrict press freedom and the right to free expression".

9.97 Dr Savage stated:

> Whilst the Strasbourg jurisprudence relating to whistleblowers (in particular *Guja v Moldova and Bucur and Toma v Romania*) is not directly applicable to journalists, the Law Commission's provisional recommendations raise important questions as to whether journalistic expression will be disproportionately restricted by the proposals. The expression rights of journalists are unlikely to be protected by allowing them to bring any information they receive from a Crown servant to an authorised disclosure route. As the Law Commission will be aware, Strasbourg provides journalists with a particularly high degree of protection to report on matters of the public interest. The practicalities of allowing journalists access to an authorised disclosure approvals process or via the Defence and Security Media Advisory ("DSMA") Notice could be further explored together with the workability of a public interest defence.

9.98 We agree with those consultees who engaged with this issue that there is little case law which guides the question of Article 10 compatibility specifically in relation to those who engage in journalistic activity. However, our discussion above suggests that, in some specific contexts, there is a real possibility that a lack of public interest defence for journalists may mean that a prosecution under sections 5 or 6 of the OSA 1989 could be incompatible with Article 10. This is especially so if the disclosed information does not relate to security, intelligence, defence or the prevention of crime.

9.99 We discuss in Chapter 11 the types of public interest defence that could be inserted into the OSA 1989 scheme in line with the recommendation that we make.

DOES ARTICLE 10 MANDATE A PUBLIC INTEREST DEFENCE?

9.100 Consultation question 22 asked:

> Compliance with Article 10 of the European Convention on Human Rights does not mandate a statutory public interest defence. Do consultees agree?

Consultation responses

9.101 In this section we analyse the consultation responses we received to this consultation question. Not every consultee responded to this point and we are grateful to those who did.

9.102 The Crown Prosecution Service agreed with this provisional conclusion without qualification. In their joint submission, the Bar Council and the Criminal Bar Association also agreed that the offences found in the Official Secrets Act 1989 do not violate Article 10 ECHR. They stated that Article 10(2) ECHR "recognises that in a democratic society there is no absolute right to disclose state secrets".

9.103 However, a large number of consultees disagreed without qualification. Some consultees including The Guardian, News Group Newspapers, Dr Ashley Savage, Campaign for Freedom of Information and Article 19, Professor Lorna Woods, Dr Lawrence McNamara and Dr Judith Townend, Dr Dimitri Xenos and Liberty argued for a variety of reasons that *Shayler* may no longer be good law.

9.104 In their consultation response, Professor Woods, Dr McNamara and Dr Townend pointed out how the case law of the ECtHR emphasises the fundamental importance of the role of the media in enabling the State to be held to account, and in turn, stresses the need to protect journalists' sources.

Is *Shayler* still good law in deciding whether Article 10 of the ECHR mandates a public interest defence?

9.105 In our Consultation Paper we were attempting to predict, based upon our assessment of both domestic law and the case law of the ECtHR, whether the Supreme Court would depart from *Shayler* were it to consider a similar case today.

9.106 Despite the criticisms made by some consultees, it is important to note that, until challenged, *Shayler* must be accepted as binding domestic authority in England and Wales. There is to date no contrary authority in domestic law, and until such authority exists, we cannot be certain whether the Supreme Court would depart from the approach it laid down in *Shayler*.

9.107 It is also important to point out that the margin of appreciation, by which the ECtHR affords the State a significant degree of latitude in cases involving certain interests, does not apply in the context of domestic law. This has been confirmed on multiple occasions by courts in England and Wales. For example, in *R v Director of Public Prosecutions, ex parte Kebilene and others*, Lord Hope observed that:

> [The doctrine of margin of appreciation] is an integral part of the supervisory jurisdiction which is exercised over state conduct by the international court. By conceding a margin of appreciation to each national system, the Court has recognised that the Convention, as a living system, does not need to be applied uniformly by all states, but may vary in its application according to local needs and conditions. This technique is not available to the national courts when they are considering Convention issues within their own countries.[645]

9.108 The courts have recognised, however, that the Human Rights Act 1998 "does not authorise the judges to stand in the shoes of Parliament's delegates, who are decision

---

645 *R v Director of Public Prosecutions, ex parte Kebilene and others* [2000] 2 AC 326 at 380H (Lord Hope of Craighead).

makers given their responsibilities by the democratic arm of the state".[646] This is not the same, however, as the margin of appreciation.

9.109 While some consultees were critical of the decision in *Shayler*, others agreed with the outcome in *Shayler* but argued it was not necessarily applicable to all offences under the Official Secrets Act 1989.

9.110 The Institute of Employment Rights, for example, stated that *Shayler* was "decided on the narrow issue of disclosures by former members of the security service under section 1(1) and should not be taken to apply to all section of the Official Secrets Act 1989". We acknowledge that.

9.111 Professor Woods, Dr McNamara and Dr Townend were critical of our reliance upon *Shayler* for a number of reasons. First, they argued that the House of Lords "cannot provide a complete answer to the requirements of the ECHR", only the ECtHR can provide an authoritative answer.[647] We are not sure that this is correct as a matter of law: the House of Lords was, and the UK Supreme Court is, binding authority on interpretation of ECHR law for the purposes of domestic law. *Shayler* is a domestic case and was not heard by the ECtHR.

9.112 Secondly, they argued that *Shayler* may be seen as a case where the relevant principles were misapplied by the House of Lords. In particular, they argued that the House of Lords' analysis of proportionality has been criticised as being inadequate, especially in light of more recent developments.

9.113 Thirdly, they argued that since the judgment in *Shayler* was handed down, the environment in which the ECtHR assesses state action has changed. Whilst the ECtHR still allows states a significant margin of appreciation, Professor Woods, Dr McNamara and Dr Townend suggest that there has been a change in emphasis in relation to the secret powers of the State and that the ECtHR now takes a much less deferential approach than in the past and that as a result *Shayler* "may not therefore represent the Supreme Court's current position".

9.114 A number of consultees expressed the view that, were the issue to come before it today, the Supreme Court would depart from the reasoning in *Shayler* and would conclude that the unavailability of a public interest defence necessarily violates Article 10 of the ECHR. (As we have already noted (see, for example, paragraph 9.5), this is not quite correct: the proportionality analysis will in fact be far more context specific, and so the court will not be asked to rule on the availability of a public interest defence in the abstract). Therefore, as many consultees including Peters and Peters as well as the Bar Council and the Criminal Bar Association noted, the key question for the Supreme Court to consider would be proportionality.

Proportionality

9.115 Many consultation responses that criticised the judgment in *Shayler* focused on its alleged misapplication of the proportionality test. Liberty, for example, characterised

---

646 *R (on the application of Mahmood) v Secretary of State for the Home Department* [2001] ACD 38, [2001] Imm AR 229 at [33].

647 L Woods, L McNamara and J Townend, para 2.14.

the House of Lords' application of the proportionality test in *Shayler* as "meagre". It relied on the views of human rights academics Helen Fenwick and Gavin Phillipson, who found that the majority decision in *Shayler* "did not consider the proportionality test in any detail, or give much consideration to the type of expression in issue".[648]

9.116 The Institute of Employment Rights similarly relied on the criticisms of Fenwick and Phillipson, noting that "*R v Shayler* did fail to consider the requirements of the proportionality test fully and this is not acknowledged by the Law Commission who also fails to examine the developments in the law on proportionality since *R v Shayler*". They argued that in our Consultation Paper we had not considered the proportionality test enunciated by Lord Sumption in *Bank Mellat v Her Majesty's Treasury (No 2),* which describes the test as it applies in the rights context in domestic law (see paragraph 9.69 above).

9.117 While we did not refer to this case in the Consultation Paper, we agree that proportionality requires a balancing of interests, which will be context specific. This was reflected in other consultation responses; Dr Xenos, for example, was also of the view that the main characteristic of the proportionality review is the need to strike a fair balance between the competing interests involved. Dr Xenos argued that "it is not possible to examine such a balancing exercise when the public interest defence that is attached to the scope of freedom of expression is not considered". He argued that the insertion of a public interest defence into the legislation is a requirement that has been confirmed by the case law of the ECtHR and specifically the proportionality analysis that is required by Article 10. Dr Xenos also argued that while the House of Lords in *Shayler* used the terms "proportionality" and "necessity", it did not apply the principles in the appropriate way.

9.118 Liberty argued that were the same issues to arise before the Supreme Court today, it would be unlikely to repeat the assessment conducted by the House of Lords in *Shayler* "of whether the current system is a necessary and proportionate interference with Article 10".

9.119 Both Prof Rowbottom and Dr Savage submitted that determining whether a prosecution for an offence contrary to the Official Secrets Act 1989 constitutes a proportionate interference with Article 10 is context-specific and is difficult to assess in the abstract. Indeed, the case law and literature reflects this. The question of whether a prosecution under the Official Secrets Act is considered compatible with Article 10 will depend on the interests to be balanced, which are only determined by the facts in each specific case. For example, where national security is the competing interest, prosecution of disclosure of information that places national security at risk may be considered a proportionate interference with Article 10.

9.120 In considering the proportionality issue, the Bar Council and the Criminal Bar Association argued that the House of Lords drew a clear distinction:

> between, on the one hand, members of the security and intelligence agencies (ie. Shayler) and duly notified persons (section 1(1)) and, on the other hand, current or

[648] H Fenwick and G Phillipson, *Media Freedom under the Human Rights Act* (OUP 2006) p 941.

former Crown servants and government contractors … whose contractual duties in this regard may be less onerous.

9.121 It was suggested that restrictions on the freedom of expression of the former would easier to justify given that absolute secrecy is a consequence of being employed by the security and intelligence agencies.

Absence of a public interest defence

9.122 Dr Dimitris Xenos in his consultation response also suggested that the House of Lords in *Shayler* did not take into account the public interest defence and did not examine the relevant case law of the ECtHR, largely because the case was decided shortly after the Human Rights Act 1998 came into force, when "the court were not very familiar with the ECHR case-law and principles, as it took some years to elaborate and apply them".

9.123 Prof Jacob Rowbottom stated that whether an external safeguard such as a public interest defence is mandated by Article 10 ECHR "will depend on the adequacy of the available internal safeguards". Prof Rowbottom argued that the case law of the ECtHR provides that "a right to go public may be justified as a 'last resort' where internal safeguards are inadequate". He argued that the conclusion expressed in Chapter 6 of our Consultation Paper assumed that "the internal channels can be made sufficiently robust".

9.124 Prof Rowbottom stated that the decisions of the ECtHR in which it has considered the Article 10 compatibility of prosecutions for the unauthorised disclosure of information can be distinguished from the current position in the United Kingdom. He stated that it is "difficult to anticipate whether the current provisions provide an adequate safeguard for every case that might arise in the future or whether the last resort of publicity would be justified in some circumstances (depending on various factors)". Given the context-specific nature of the case law of the ECtHR, Prof Rowbottom stated that it is difficult to rule out the Court concluding that disclosing information publicly was justified in some future case.

9.125 Whilst the ECtHR accepts that in principle an employee should seek to use internal procedures before making a public disclosure, this does not require employees to use systems that are 'clearly impractical'. Professor Woods, Dr McNamara and Dr Townend noted that the Court in *Guja* clarified the possible meaning of "impractical" and "last resort" as "whether there was available to the applicant any other effective means of remedying the wrongdoing which he intended to cover". Professor Woods, Dr McNamara and Dr Townend then took the view that the test for effectiveness should therefore "be understood similarly to that used in the context of the requirement to exhaust local remedies in the Convention; that is, they are capable of providing redress in relation to the particular situation at hand". Given this approach, they questioned whether internal mechanisms alone could ever pass this test. As an example, they noted a statement made in the report on *Leaks and Whistleblowing in Whitehall* by the Public Administration Committee in 2009[649] where those civil

[649] Leaks and Whistleblowing in Whitehall, Report of the Public Administration Select Committee (2009) HC 83.

servants who provided evidence "did not have much faith in internal whistleblowing procedures".

9.126 In relation to whether it is necessary to exhaust these internal processes before a disclosure is made, Professor Woods, Dr McNamara and Dr Townend submitted that, following *Heinisch v Germany* (see paragraph 9.39 of this Report), this criterion of exhausting internal processes should be understood as just one of six and not as a requirement that must be satisfied before the other criteria are considered. In turn, they argued that to require a whistleblower to exhaust internal mechanisms before disclosing, or to use only those internal mechanisms, "would be likely to be disproportionate".

9.127 In their joint submission, Campaign for Freedom of Information and Article 19 argued that the effect of *Guja* and *Bucur* (see paragraphs 9.40 to 9.42 of this Report) was that:

> If the internal mechanism fails, disclosure of information of public interest including classified information … is protected under Article 10. Thus, in Convention law, there is a de facto public interest defence and any new legislative measure which fail to recognise this would not be in compliance with the European Convention on Human Rights, and the Human Rights Act 1998.

9.128 Dr Savage stated that whilst the ECtHR makes reference to the importance of official mechanisms, "it also makes clear that individuals can be protected by Article 10 where these mechanisms have failed or are not viable to rely upon in the circumstances".

9.129 It was clear from the consultation responses that, although the existence of effective internal mechanisms is an important element in the compatibility of offences with Article 10, a public interest defence could ensure compatibility where those mechanisms fail. This has also been argued for in the literature; Kagiaros for example has argued that the state "would have to counterbalance the absolute ban on external disclosures by establishing a robust system of independent and effective internal mechanisms" but also noted that:

> even if such mechanisms exist, they do not suffice to bar the whistleblower from proceeding to a public disclosure and courts from proceeding to the ad hoc test of whether they functioned properly in that particular instance and whether the disclosure was in the PI. [This] approach therefore, does not provide an adequate solution to the problem of balancing the interests of security and disclosures.[650]

9.130 We agree with the common view that while Article 10 does not mandate a public interest defence, the existence of such a defence will make it even less likely for an offence under the Official Secrets Act 1989 to be incompatible with Article 10, even where internal mechanisms are made available.

---

650 D Kagiaros 'Protecting "national security" whistleblowers in the Council of Europe: an evaluation of three approaches on how to balance national security with freedom of expression' (2015) *The International Journal of Human Rights* 19(4) p 416.

The lack of a public interest defence and its impact on Article 10

9.131 As a number of consultees pointed out, the lack of a public interest defence would be most likely to be relevant in determining whether a fair balance had been struck between the rights of the individual being prosecuted and the interests of the community. The court would not consider the issue in the abstract but would have regard to the facts of the case to assess whether the interference with the defendant's right to freedom of expression struck the fair balance required by the proportionality test. Of relevance would include the following factors: whether the defendant was a Crown servant, government contractor or member of the security and intelligence agencies; the nature of the information that was disclosed without lawful authority; the motivations for disclosing the information; the extent to which any damage was caused to a protected state interest; the extent to which the defendant first relied upon internal grievance measures or sought approval to disclose the information; and the public interest in disclosing the information.

9.132 It was argued by Professor Woods, Dr McNamara and Dr Townend that:

> … the lack of a public interest defence, would be a factor in any analysis seeking to balance, on the one hand, the whistleblower's rights to freedom of expression and the corresponding right of the public to receive that information, and on the other, the public interests sought to be protected by restricting the information.

9.133 It was argued therefore that the inclusion of a case-by-case public interest defence would be a more "targeted", and in turn proportionate, response. This was on the basis that a public interest defence operating in this way would allow "space for the interests of the whistleblower, journalists and audience" alike.

9.134 Liberty noted that the ECtHR had found "in many cases that sanctions against public interest whistleblowers breached Article 10", citing *Matúz v Hungary*[651] and *Wojtas-Kaleta v Poland*[652] and arguing that, while we had cited this case law in part, we failed "to examine its clear and crucial implications for whistleblowers".

9.135 In his consultation response, Dr Savage stated that whilst the case law of the ECtHR:

> does not mandate a public interest defence, it makes clear that where information is of a sufficiently high value to outweigh competing interests (to the organisation) and attempts to raise the concern through authorised channels have failed or it is not practical in the circumstances to do so an individual is able to obtain protection under Article 10.

9.136 Similarly, while disagreeing with the provisional conclusion, the BBC concluded that:

> [a]lthough we agree that case law does not currently mandate a freedom of information defence, the cases repeatedly stress the importance of Article 10 and we therefore believe that such a defence is desirable.

---

651 *Matúz v Hungary* [2014] ECHR 1112.

652 *Wojtas-Kaleta v Poland* 20436/02 [2009] ECHR 1120.

9.137 The Institute of Employment Rights argued that:

> the enactment of a statutory public interest defence would ensure compliance with the Convention right to freedom of expression, protecting both investigative journalism and whistleblowers who disclose information in the public interest. Any bill failing to provide a public interest defence misses an opportunity to protect the human rights of whistleblowers.

9.138 In their consultation response, Peters and Peters argued that the absence of a public interest defence might prevent important issues that relate to the ideals that are important to a democratic society from being considered when evaluating whether an offence has been committed. Thus, it suggested that excluding a public interest defence may be disproportionate "especially if the 'legitimate' routes for whistle-blowing fail to result in the matter being dealt with appropriately".

9.139 What we can say with confidence based upon consultees' responses and our own analysis in light of the existing literature is that the lack of a public interest defence is a factor that would be relevant to an assessment by the ECtHR of whether the interference with the defendant's right to freedom of expression was proportionate. Depending upon the precise circumstances of the unauthorised disclosure, the lack of a public interest defence *could* lead to the conclusion that a prosecution constituted a violation of Article 10. In some cases, the lack of a public interest defence could be the determinative factor, especially where a public disclosure was made as a "last resort" in the absence of effective internal mechanisms to address alleged wrongdoing.

9.140 It has been argued in the academic literature that a blanket ban on disclosure, without any availability of a public interest defence, may compromise the liberalising nature of the legislation that was presented on its enactment. Helen Fenwick, for example, notes that:

> the information may concern corruption at such a high level that internal methods of addressing the problem would be ineffective. Clearly, good intentions are normally irrelevant in criminal trials … However, it is arguable that an exception to this rule should be made in respect of the Official Secrets Act. A statute aimed specifically at those best placed to know of corruption or malpractice in government should, in a democracy, allow such a defence. The fact that it does not argues strongly against the likelihood that it will have a liberalising impact.[653]

9.141 Similarly, Vickers states that "the absence of any public interest defence … undermines any claim that the 1989 Act represents the liberalisation of the UK's laws, and the freedom of speech of civil servants remains significantly restricted as a result",[654] an argument expressed by other academics in the field such as Fenwick and Phillipson.[655]

---

653 H Fenwick (2017) Civil Liberties and Human Rights p.506-507.

654 L Vickers (2002) Freedom of Speech and Employment p 211.

655 See, for example, H Fenwick and G Phillipson (2007) Media Freedom under the Human Rights Act, H Fenwick and G Phillipson (2017) Text, Cases and Materials on Public Law and Human Rights.

9.142 We have departed from the view we expressed in our Consultation Paper to the extent that we agree with consultees that the unavailability of a public interest defence *may* lead the Supreme Court or the ECtHR to conclude that a prosecution for an official secrets offence constituted a disproportionate interference with the right to freedom of expression enshrined in Article 10 of the ECHR. In the domestic law context, we cannot be confident that the Supreme Court would invariably follow the approach that was taken in *Shayler* in all factual scenarios, especially since, as a number of consultees pointed out, the proportionality test as it exists in domestic law today is more rigorous that the one applied by the House of Lords in 2002.

CONCLUSION

9.143 In order for an interference in freedom of expression to be compliant with the ECHR, the interference must be prescribed by law, pursue a legitimate aim, and be necessary in a democratic society. For our purposes, the first two limbs are relatively uncontroversial. It is the third limb – assessing whether the interference goes further than necessary in meeting the legitimate aim – that has required more detailed consideration.

9.144 We began by asking what minimum qualities the interference (prosecution/threat of such) must possess in order to be compliant with Article 10. It is clear from long-standing Strasbourg jurisprudence – from *Klass v Germany* to *Catalan v Romania* – that an interference will be likely to be proportionate so long as it does not remove the possibility for effective redress of serious wrongdoing. States are rightly afforded a wide margin of appreciation in determining how best to counter threats to national security, which may include imposing legal duties of confidentiality, but there must be adequate safeguards against abuse of these measures. For example, states cannot use the cloak of confidentiality to disguise illegality.

9.145 However, the ECtHR has repeatedly emphasised the duty of loyalty and confidentiality owed by public servants to their employers. Where there exists an effective forum for redress – whether in statute or practice (e.g. reporting to superiors) – the ECtHR has not looked sympathetically on those who disclose to the public in breach of their duty without first exhausting these mechanisms (see, for example, *Catalan v Romania*, at paragraph 9.36 above).

9.146 These mechanisms must, however, be *effective*. The mere existence of legislation will be no guarantee that, in the circumstances of a particular case, there existed effective means of redress.

9.147 The reverse formulation is also true. It is worth emphasising, as Lord Hope did in *Shayler* and as is evident from all of the Strasbourg case law above, that the Court will consider the question of compliance by taking into account all the circumstances of the case in question. So, the absence of an effective mechanism for investigation and redress or a public interest defence will not, in and of itself, mean that a state has failed to comply with its Article 10 obligations.

9.148 The ECHR does not, therefore, mandate any specific form that Article 10 protections must take, just as it does not mandate any specific form that the mechanisms for redress must take. What is clear is that a public servant will be afforded protection under Article 10 for public disclosures of serious wrongdoing as a last resort – where

there did not exist any other effective mechanism for investigation and redress. It is significantly less clear that such protection will be extended to those who disclose to the public without having used such mechanisms.

9.149 The ECHR does not mandate a public interest defence for journalists either, though, as we have seen, there are plausible scenarios where the ECtHR might hold that a public interest defence was necessary. Given their lack of prior duties of loyalty, reserve and discretion, journalists may be afforded greater latitude than public servants in exercising their Article 10 rights (and, given this, it would be difficult to *mandate* that journalists report first to a state body, such as the statutory commissioner we recommend in the following chapter).

9.150 We have made clear that Article 10 does not impose an obligation on member states to disclose information. Further, public disclosure of abuse (eg where secrecy was used to hide illegality) is not directly mandated by Article 10. This is to say, a disclosure may be afforded protection on the basis that it is in the public interest, but that does not equate to protecting *public* disclosures, merely because the disclosure was in the public interest (this could be achieved by, for example, reporting to the CPS). The state must demonstrate that it has adequate safeguards in place to prevent abuse of laws which interfere with the right to freedom of expression, such as mechanisms for effectively reporting and investigating wrongdoing. Nothing in Article 10 explicitly requires that these safeguards operate wholly in the public domain – Article 10 is about freedom of expression, and does not mandate government transparency. (This is not to deny, however, that some element of transparency may be required in order to ensure that the safeguards operate effectively in the first place).

9.151 We have also made clear that there is a real possibility that *Shayler* would be decided differently were it to come before the Supreme Court today.

9.152 What we therefore propose is a regime for protecting official data that will make it more likely that, in any given case, the UK will be found compliant with Article 10.

9.153 Our recommendations are as follows:

(1) An independent commission should be created by statute, with broad powers to investigate disclosures of wrongdoing. This reflects not only our view that this would be necessary to ensure adequate protection to public interest disclosures for the purposes of Article 10 and domestic law, but also the broader principle that the cloak of confidentiality should not be used to mask serious wrongdoing.

(2) We recommend a public interest defence for public servants as a last resort. We recognise that the cases in which that defence might be advanced may be the rare cases when our proposed statutory commission would not constitute an effective investigative mechanism for the purposes of Article 10. For example, in the chapter on the statutory commissioner, we consider that the urgency of the complaint could, in extreme cases, mean that unauthorised public disclosure is in the public interest and thus will be afforded protection under Article 10. We should be clear that we are not saying that the public interest will justify disclosure in all cases of urgency. Rather, we are saying that it is conceivable that the urgency of the complaint *may* mean that, in some cases,

unauthorised disclosure was justified. We also consider that there may be instances where, despite its independence, a conflict of interest may preclude effective investigation of the complaint by the statutory commission.

(3) We also recommend a public interest defence for journalists and others charged under sections 5 and 6 of the Official Secrets Act 1989.

(4) We make no recommendation as to the precise form such public interest defences should take, other than that they should be available to all those charged with offences under the 1989 Act. It would be open to the defendant to prove that their disclosure was in the public interest, both in terms of manner and content. A limited public defence available to the defendant in court, whether or not that defence succeeds, makes it considerably less likely that the UK will be found not to be compliant with Article 10.

Chapter 10: Recommendations for an Effective Investigative Mechanism

10.1 The law needs to afford adequate protection to official secrets while ensuring the UK meets its obligations under Article 10 ECHR. There is a clear public interest in the ability of the government and the intelligence, defence, and security agencies to protect the public. It is evident that real damage can be caused by unauthorised disclosures, both to national security and to individuals. However, it will be recalled from our chapter on Article 10 that we cannot guarantee that the Official Secrets Act 1989 ("OSA 1989") will, in all instances where the law prohibits public interest disclosure, comply with the requirements of Article 10.

10.2 To help achieve a balance between affording proper protection to official data and allowing appropriate investigations of alleged impropriety, we recommend that those who fall within the ambit of the offences in the OSA 1989 ought to be able to raise concerns about serious wrongdoing to an external, independent investigative body. They should be able to do so anonymously (if they wish) and without risking criminal liability under the Official Secrets Acts or equivalent offences. Disclosures that would otherwise be criminal will not be so if made to this body in accordance with its processes. The independent body would then come under a duty to investigate.

10.3 Consultees responding to the provisional proposal for a statutory commissioner were generally opposed to that model if presented as an alternative to a public interest defence, though a number of consultees agreed that a new statutory commissioner model would be more effective than the current reporting regime.

10.4 In light of consultees' responses and the analysis of Article 10 in the preceding chapter, we consider not only the statutory commissioner model (with a developed idea of how that would operate) but also how a public interest defence would sit alongside the statutory commissioner model, as a mechanism of last resort. We make recommendations for both.

THE STATUTORY COMMISSIONER AND CONSULTATION RESPONSES

10.5 It will be recalled from Chapter 8 that there was some support from a diverse range of consultees for an external, independent body to receive and investigate complaints of wrongdoing (albeit that some consultees did not consider a statutory commissioner alone to be sufficient absent a public interest defence).

10.6 Consultees also shared our view that the existing routes for disclosure – including the Civil Service Commission, the Ethical Counsellor, the Director of Public Prosecutions and the Intelligence and Security Committee – were insufficiently expeditious, insufficiently independent, and insufficiently equipped to conduct the necessary investigations.

10.7 We also noted that a statutory commissioner model must have certain attributes if it is to achieve its purpose. We noted that meaningful independence means that the office-

holder must have security of tenure to insulate him or her from improper influence. We also noted that the commissioner must have sufficient powers of investigation (such as the legal power to compel disclosure), and the ability to employ those powers expediently and within all reaches of the intelligence and defence services. To that end, it is important that the commissioner has experience of and a relationship of trust[656] with the intelligence and defence services, whilst retaining independence.

The Investigatory Powers Commissioner's Office ("IPCO")

10.8 In our Consultation Paper, we proposed augmenting the function of the Investigatory Powers Commissioner's Office ("IPCO") to take on this role. It was our view that IPCO would be well-placed to investigate concerns of wrongdoing, given its existing jurisdiction, independence and investigative reach with respect to the UK intelligence community. A number of consultees agreed that the UK system for disclosures would benefit from independent oversight, and many agreed provisionally, and subject to the final form of any such recommendation, that IPCO would be well-placed to undertake the role.

10.9 We are confirmed in our provisional view that a statutory commissioner should form an essential part of future compliance with Article 10, and that IPCO is well-suited to the task. Of course, whether IPCO should further assume the role of the statutory commission would have to be a matter for government – we make no recommendation in this regard. It would also have to be adequately resourced (though this is true of any effective investigative mechanism). We note the role of IPCO here merely to demonstrate that frameworks exist that make the statutory commission a real and tangible possibility.

10.10 The Investigatory Powers Commissioner is supported by a number of Judicial Commissioners, who are highly experienced, former senior members of the judiciary, including former High Court, Court of Appeal and Supreme Court judges. Their governance arrangements, in ensuring independence from government, are therefore both effective and reliable. Alongside judicial expertise, IPCO has a team of almost fifty staff – including investigators, lawyers, and communications experts – who have established connections and trust throughout the security and intelligence services (amongst many others) as well as expertise in holding them to account.

10.11 All intrusive powers of investigation – from interception, equipment interference and surveillance – are subject to the approval of a Judicial Commissioner. This is work that often requires decisions on very tight timetables.

10.12 Further, under section 235 of the Investigatory Powers Act 2016, IPCO already has the legal authority to compel disclosure of "such documents and information as the Commissioner may require for the purposes of the Commissioner's functions." This would include the power to compel disclosure of documents held by the security and intelligence services.

---

656 To this end, IPCO's annual report affirms IPCO's guiding principles which include, amongst others, both transparency but also – relevantly – that IPCO will not itself be the source of improper disclosure of secret information. *IPCO Annual Report 2017* (2019) HC1780p 8.

10.13 It will be recalled that we considered that the statutory commissioner would have to be independent, effective, and trusted. This would require independence from Government, security of tenure and the ability (practical and legal) to conduct expedient and rigorous investigations. We remain of the view that IPCO satisfies these requirements. The remit of IPCO is already sufficiently broad to accommodate the role we envisaged in the Consultation Paper. Given its statutory mandate, IPCO already has the infrastructure necessary to perform this role.

10.14 We acknowledge that the Investigatory Powers Act, which created IPCO, only received Royal Assent in 2016. As consultees pointed out, IPCO is a newly-established institution. This necessarily makes it more difficult to gauge its long-term performance. There are clear indications, however, that the Investigatory Powers Commissioner fully recognises the need for IPCO to be a more public-facing institution than the ones it has replaced. In contrast to the view taken by consultees, we believe that the fact that IPCO is so newly-established is a point in its favour. This increases the possibility that it will be open to adopting new ideas and expanding its remit. It also reduces the possibility that people have a jaundiced view of the commission as a body that holds entrenched views which would be difficult to displace. In any case, any new body would face the same or greater difficulties with respect to its limited track-record.

10.15 Given that the office has already been established, we do not believe that relying upon IPCO to receive and investigate concerns would add unnecessary bureaucracy. There is no need for legislative amendment to the OSA 1989, as disclosures which are made to IPCO already constitute authorised disclosures.[657]

10.16 As consultees pointed out, should the role of IPCO be expanded to include receiving and addressing concerns that would otherwise involve unauthorised disclosures under the OSA, it would be essential for appropriate resources to be devoted to this element of its work. This role must be given the attention it deserves and not perceived to be less important than the other statutory functions IPCO is required to discharge.

10.17 We remain of the view that IPCO would, with some expansion of its role and some amended powers and resources, provide an effective means of ensuring that concerns about potential wrongdoing are effectively investigated by an independent and rigorous oversight body.

10.18 Nonetheless, whether or not IPCO assumes the role of the statutory commission, it is necessary to discuss in detail what the commission model should be.

WHAT WOULD THE STATUTORY COMMISSIONER MODEL LOOK LIKE?

Who can make disclosure to the Statutory Commissioner?

10.19 Whilst the Consultation Paper focussed on public servants, we consider that the statutory commissioner ("the SC") would be able to receive concerns about serious wrongdoing from both public servants (Crown servants and government contractors) and members of the public. The most relevant section of the public would be the media, as they are the people most likely to be in possession of official data subsequent to an unauthorised disclosure by a public servant. Anyone who risks

657 Section 237 of the Investigatory Powers Act 2016.

committing an offence under the 1989 Act would be entitled to make a disclosure to the SC.

10.20 We agree with stakeholders that it is important that concerns are capable of being raised anonymously, should the person making the disclosure not wish to divulge their identity. This matter could be addressed both through guidance and through use of technology. (In this respect, it is worth noting that IPCO has a Technology Advisory Panel that could facilitate anonymous reporting). We recommend that provision be made for anonymous reporting, after consultation on how that can best be achieved and on what guidance needs to be provided to ensure confidence in the anonymity of the process. A consultation would provide the relevant stakeholders with a further opportunity to give their views on how this mechanism could be made as effective as possible.

10.21 Where there is a risk that an investigation will result in the complainant's identity becoming known within the Department or agency about which the complaint or concern has been raised, despite the SC's best efforts, then the complainant and the SC between them may have to consider whether and, where appropriate, how an investigation should be undertaken.

Evidence requirement

10.22 In one sense, this should be self-evident: the purpose of the SC – as we envisage it performing the role we are creating – is to receive disclosures of confidential information to investigate them. However, it is worth making clear what this will exclude from their scope of responsibility.

10.23 It is envisaged that the SC would only investigate those concerns that are:

(1) supported by evidence (whether tangible evidence or credible reports); and

(2) where the substance of the allegation is not in the public domain.

10.24 If there has already been a disclosure to the public – authorised or not – then there are more appropriate authorities to conduct formal investigations of wrongdoing (such as, for example, the police). There are, for example, bodies that have search and seizure powers or general arrest and investigation powers, and are therefore better-placed to conduct formal investigations.

10.25 Instead, the purpose of the SC in this role would be to ensure that confidentiality is not being used within Government as a cloak to mask serious wrongdoing. Where there is evidence that an agency or public servant may be engaged in wrongdoing, the SC would serve to effect appropriate redress (that may include public disclosure and passing evidence to a prosecutorial body). Crucially, it would do so in such a way as to minimise, so far as possible, unnecessary harm to the public interest. The assessment of the public interest would unavoidably include an assessment of the potential harm to public servants or the proper duties thereof that a disclosure would cause.

10.26 The bare requirement that an application is supported by evidence is not a particularly high bar, but precludes from the scope of the SC's duty unsubstantiated requests for investigation. Its function would be to investigate evidenced allegations of wrongdoing,

not to act as a conduit for public curiosity (however sincere). We consider that this would meet some of the risk that the SC would be deluged with requests from members of the public, though concede that some level of risk remains if members of the public are permitted to use the SC.

The SC's duty upon receiving a complaint

10.27 In order to understand the nature and scope of the SC's duty upon receiving a complaint, we need to reiterate why it is suggested that an external body such as the SC is required in the first place.

(1) The main legal reason for proposing an SC is based on our understanding of the Article 10 jurisprudence. To attempt to prohibit all public disclosures of information protected by the OSA is likely to be incompatible with Article 10, particularly where what is to be disclosed is serious wrongdoing. Some Article 10 cases have recognised that public disclosure is the only effective remedy. The SC will ensure that there is always a route of disclosure that will prompt effective investigation of wrongdoing.

(2) We also have evidence from consultees that an independent channel of reporting would be welcomed by those public servants who may have legitimate concerns about wrongdoing but who would not ideally wish to make public disclosure. As noted previously in this Report, Annie Machon has long campaigned for this.

10.28 Given this need, what functions should the SC therefore perform as a bare minimum?

(1) Given the legal basis for the SC, the minimum function it should perform is to effect meaningful investigation of alleged wrongdoing – "meaningful" in the sense that it leads to some form of remedy if wrongdoing is made out.

(2) As a practical consideration, it needs to investigate the complaint sufficiently to be able to determine its veracity and to come to a judgement on how best to effect that redress. So, the duty to conduct some sort of investigation is not really in doubt.

10.29 The SC could, we envisage, be placed under a statutory duty to investigate complaints by those subject to the OSA 1989 where to make the complaint publicly would involve making an unauthorised disclosure. The SC would have a duty to determine whether the complaint has a basis in fact and, if necessary, to effect remedy.

10.30 However, it is worth noting that public disclosure *by the SC* of any conclusions reached in its investigation is not directly necessitated by Article 10. The bare minimum is that wrongdoing is not allowed to go unchecked. Confidentiality cannot be used to mask wrongdoing, but that does not mean that the only remedy for wrongdoing is an immediate *public* unmasking. We consider this matter in detail below, along with the possible range of outcomes following an SC investigation.

10.31 We did not consult on what specifically constitutes 'serious wrongdoing' and 'public interest', and we make no recommendations in this respect. We consider that it would be appropriate for Parliament to determine the content of these terms on the basis

that such a determination is, at least in significant part, a question of policy. For the avoidance of doubt, this is not to suggest that the government of the day can determine the content of these terms as they see fit. Rather, it did not fall within the scope of our consultation to define these policy terms, and further consultation is necessary.

Outcome of investigation

10.32 In this section, we consider the range of options available to the SC following an investigation of a complaint. We consider the matter of public disclosure first, given that, as will become clear, this must be considered alongside whatever other remedy is pursued. We further consider what matters might inform the form and content of that disclosure. We then consider other remedial actions.

10.33 It should be noted, for the avoidance of doubt, that whatever proper disclosures of sensitive information the SC makes as a result of its receiving a complaint should not constitute an offence under the OSA 1989. Of course, unauthorised disclosures of this information by the statutory commissioner or SC staff should still constitute an offence.

Public disclosure by the SC

10.34 It will be recalled that Article 10 does not, in and of itself, mandate public disclosure. If public disclosure of complaints is not directly necessitated by Article 10, is public disclosure in some form by the SC indirectly necessitated?

10.35 For the avoidance of doubt, the discussion at this stage of the necessity of public disclosure by the SC does not mean specifically disclosure of the evidence. Disclosure may involve disclosure of that evidence, but it may involve both greater and lesser disclosure, and may involve different types of disclosure to different bodies. We therefore stress that we are first considering whether public disclosure is necessitated *in some form*. We consider later what may be required of the content of that disclosure.

10.36 In answering this question, it may be helpful to consider the extreme alternative. What if the SC never made any public disclosures or comments and only ever passed on its findings to other bodies, such as the Prime Minister or the Intelligence and Security Committee of Parliament ("ISC"), or at least effected whatever internal remedy it could? Would that have negative consequences and could it satisfy Article 10?

(1) On the one hand, this would not be problematic: public disclosure is arguably not an end in itself (or certainly not solely an end in itself), but serves to shine a light on (and so help prevent) impropriety. If the SC had found other methods to achieve that objective, then it is not obvious that this would be a problem.

(2) On the other hand, there is the question whether the complainant should be made privy to some sort of information from the SC following the investigation into their complaint? There is at least one significant reason for thinking they should. There would be little incentive for concerned Crown servants and others caught by the OSA 1989 to make disclosures to the SC if they felt they were just shouting into the void. There needs to be some feedback loop to ensure that people feel that their complaints have been taken seriously.

(3) The SC would also risk accusations of being insufficiently transparent. By way of comparison, it is worth noting that one of IPCO's guiding principles is transparency,[658] meaning that material that can properly be made public ought to be available for scrutiny. One of the significant advantages of an independent, external investigator is its ability both to hold to account and to be seen to hold to account the security and intelligence community. Whilst the ISC is independent in the sense that it is both cross-party and broadly independent of government, it is not independent of Parliament. Our concern, if the SC were to serve a purely investigative function with no mandate for public disclosure, is that the public perception of the process will be that it is 'internal' rather than external (albeit that this might not be true in the narrow sense). There would thus be reputational risk to the SC generally if it were seen to be operating "within the shadows" rather than as an external, independent reviewer.

(4) This perception may, in turn, mean that the SC is not regarded as an effective investigative mechanism, and that would undermine the entire regime.

10.37 There is therefore a strong argument that there should be some form of disclosure by the SC (though not necessarily full public disclosure, or disclosure of otherwise protected material), without prejudice to any other remedies it may consider appropriate.

10.38 This may be limited to public disclosure of an investigation into alleged impropriety. It is worth noting that this conforms with the Investigatory Powers Commissioner's ethos of transparency, so were IPCO to assume the role of the SC (though we make no recommendation in that regard), that mitigates the risk of undermining its objectives and function by appearing distant and opaque.

What form should public disclosure take?

10.39 As we have noted, in order to fulfil its function in ensuring that, in so far as it is possible to predict, the UK does not risk contravening Article 10, the SC would have to facilitate effective investigation of wrongdoing. We have already recommended that, following investigation of a complaint, the SC would have to make some form of public disclosure. However, it is necessary to determine what the content of that disclosure might be and to whom that disclosure should be made.

10.40 The SC will have to determine what form and content of disclosure best meets the public interest in the particular case. The public interest in the content of the disclosure will be determined in significant part by the nature of the information revealed by the investigation. It will generally be in the public interest to make known (in one form or another) results of investigations that reveal serious wrongdoing. This confirms the approach of the European Court of Human Rights, which has repeatedly emphasised that freedom of expression will warrant protection under Article 10 where confidentiality is used as a way of masking wrongdoing. It is in the essence of the SC

658 *IPCO Annual Report 2017* (2019) HC1780 at [2.3]

model that serious wrongdoing can be aired publicly and accurately (with as little damage to proper administration of government as is possible).

10.41 It is not so obvious that there would be a sufficient public interest in the disclosure of Governmental wrongdoing which is of a type which although it may be politically controversial is not otherwise illegal or demonstrative of wrongdoing. Consider, for example, where the government choose to pursue a defence or security strategy on the basis of the advice of their own specialist advisers, but where that advice is contested. It is not difficult to construct an argument that there may be some public interest in this information in the abstract, but it is more difficult to construct an argument that there is a sufficient public interest to share that information where to do so risks undermining national security and trust between intelligence partners. In any case, the mere fact of a policy being controversial should not be enough to invite public scrutiny: strategic decisions have to be made on contested or contestable evidence all the time, and it would be fanciful to suppose that there was a public interest in their disclosure merely because of the contested nature of the evidence.

10.42 More significantly, there comes a point at which the jurisdiction of the SC should not extend to questioning the proper policies of Government and Parliament. We have not consulted on how the public interest could be determined in any given case, so we cannot specify the SC's jurisdiction in concrete terms, beyond recommending that it should extend to investigating wrongdoing and to publishing its findings. Its focus should not be on challenges to policy judgments made by Government. It is, of course, conceivable that the formulation of a policy, or a policy itself, may involve wrongdoing, but then it is the wrongdoing itself that attracts the jurisdiction of the SC. The final say on the proper jurisdiction of the SC would be for Parliament to determine in appropriate legislation.

10.43 Though we have not consulted on the content of the term "public interest", and so we cannot recommend a full list of factors that the SC may consider when judging the form and content of disclosure, we note that the following are possibilities.

(1) Where the SC's investigation does not uncover wrongdoing, then the disclosure may be limited to a confirmation that a complaint was received and an investigation was undertaken that revealed no wrongdoing. The extent to which the SC chooses to elaborate on the nature of the investigation (which was the relevant agency, for example) or on the nature of the complaint (what was the allegation) will be a matter for the SC considering the public interest in transparency and the risk that even that publication may pose to national security. We also recommend that it reports on the numbers of cases investigated in an annual statement to the Prime Minister and ISC.

(2) If the SC's investigation does reveal wrongdoing the position is more difficult. We consider that there are a number of options for disclosure that the SC could be tasked with performing. The Government should examine the desirability of these when establishing the SC and providing its full terms of reference. They include, but would not be limited to, one or more of the following:

(a) authorise the complainant to make disclosure in full or redacted form;

(b) disclose the original material on its own or in conjunction with material uncovered from the investigation, each in full or redacted form; and

(c) submit a dossier of evidence to the appropriate prosecutorial body (if the wrongdoing amounted to a crime).

(3) We consider that it is important to allow the SC the possibility of authorising the original complainant to make the disclosure if it is in the public interest so to do. This would be especially important where, in an unusual case, the complainant who has lodged the concern with the SC is a journalist. Though we are confident that editorial priorities should not form part of the public interest test (the public interest is not determined by a private publishing interest), that does not mean that the interest a person has in making comment should be ignored if disclosure is in the public interest.

(4) Where the disclosure is extensive or complicated, or cannot be made without disclosing further sensitive information uncovered by the SC, it may be more appropriate that the SC disclose the information in a report of its own.

(5) We do not envisage that the SC would be a prosecutorial body. Where its investigation yields evidence of a crime, the SC should submit evidence to an appropriate law enforcement or prosecutorial body such as, for example, the Metropolitan Police Service or the Crown Prosecution Service. In such circumstances, it will be necessary to consider the implications of so doing: the disclosure of potentially highly confidential information will have to be managed with extreme care. It is likely that there will have to be a protocol in place between the SC and the relevant body to ensure appropriate handling of information and that staff who have access to the information are appropriately vetted. Without such protocols in place, there is clearly a risk of further breaches of the Official Secrets Acts.

(6) A public interest in public disclosure does not imply a public interest in *immediate* disclosure. There may be very good reasons for withholding evidence of wrongdoing if such disclosure would risk harm to entirely legal and proper activities. This would be unlikely to be appropriate in the case of ongoing wrongdoing, where prevention of the wrongdoing would feature highly in any consideration of the public interest. Nonetheless, the SC would have also to consider the timing of disclosures in its estimation of the public interest.

Other remedial actions

10.44 Even if necessary in all cases, disclosure is a remedial tool and not an end in itself. While some other forms of remedy may fall outside the SC's jurisdiction (such as the decision to prosecute for a criminal offence), some ought properly to fall within.

10.45 For example, IPCO already has the power under section 7 of the Investigatory Powers Act 2016 to impose monetary penalties for unlawful interception of communications. This is a power that it assumed from its predecessor. IPCO also has a number of powers in respect of its function in authorising and auditing the use of investigatory powers (such as, for example, refusing to grant or withdrawing the approval of a warrant). As we have not consulted on what constitutes wrongdoing for these

purposes, it would not be appropriate or helpful to speculate further on what types of action would warrant this form of sanction. For now, however, it is worth noting that there is a legislative and practical framework in place enabling this form of redress for wrongdoing.

Reporting to the ISC and to the Prime Minister

10.46 Without prejudice to our view on public disclosure, we also recommend that the SC should lay its final reports on investigations before the ISC and the Prime Minister to ensure that it is meeting its duty. This is much the same way that IPCO is currently under an obligation to report to the Prime Minister. We considered in the Consultation Paper whether reporting solely to the executive was an appropriate safeguard. Our provisional view is that the SC ought to make a report to the ISC as well to the Prime Minister, given that the ISC takes its membership from across both Houses of Parliament. This ensures a further level of scrutiny that is external to government.

10.47 We do not consider that it would, in all circumstances, be appropriate to make a detailed report of the investigation. This would especially be the case where no wrongdoing was uncovered. It may be sufficient that the ISC and Prime Minister have oversight of the number of investigations that have been undertaken and generalised data on the outcomes of those investigations.

10.48 Where wrongdoing has been uncovered, and without prejudice to other forms of redress including public disclosure, it would be appropriate to submit a full report to the ISC and to the Prime Minister, save where the public interest militates against such a strategy (where, for example, a member or members of the ISC are implicated in the wrongdoing).

TIME-SENSITIVE COMPLAINTS

10.49 Compliance with Article 10 requires that mechanisms exist that allow for effective investigation and redress of wrongdoing. One necessary element in determining the effectiveness of these mechanisms is that the SC can act in an appropriately timely fashion, relative to the complexity, urgency, and importance of the complaint.

10.50 There is also a distinction to be drawn between initiating an investigation in an appropriately timely fashion and making a public disclosure in an appropriately timely fashion. It does not automatically follow that an immediate problem requires immediate public disclosure, even if it warrants immediate investigation.

10.51 Our reasoning is as follows. Allowing wrongdoing to be made public serves the public interest in two related ways. First, it allows justice to be done in affording visibility to wrongdoing that may otherwise remain confidential, and in doing so ensures that it can attract appropriate criminal or regulatory sanction. Secondly, that threat of sanction and public censure may prevent current wrongdoing or deter future wrongdoing. The knowledge that there will be a body with the clearance, expertise and networks to investigate the full reaches of the security and intelligence services means that those agencies will be aware that their wrongdoing could become known and so command public censure and criminal sanction.

10.52 However, these aims are only achieved if there is real and credible evidence sufficient to warrant criminal or regulatory sanction. To this end, the mere fact of a public disclosure will not, in and of itself, achieve anything. Making unsubstantiated evidence public, prior to any formal investigation, may afford wrongdoers time to conceal or destroy further evidence. In allowing justice to be done or preventing wrongdoing, public disclosure is not the end in itself, but a means to an end. If the sole purpose of a public disclosure were to prompt an investigation, when there existed a mechanism for investigation that would have included – where necessary in the public interest – a public disclosure, one may rightly ask why we should countenance the risks attendant to such a disclosure. These risks include the risk of frustrating any future investigation.

10.53 This does not, of course, preclude the possibility that the SC may be unable to respond in a sufficiently timely manner. In these cases, we consider that it might be open to a defendant who had disclosed material to prove that they were acting in the public interest in making a disclosure directly to the public.

CONFLICTS OF INTEREST

10.54 This is a problem that may or may not arise, depending on the model of statutory commission that is adopted. One of the difficulties with expanding the role of IPCO to assume the duties of an SC is the potential for a conflict of interest. IPCO's primary role is in relation to the scrutiny of warrants issued under the Investigatory Powers Act 2016. A potential problem arises where the issue of alleged impropriety or illegality which the Crown servant wishes to raise relates to such a warrant. A report to the Commissioner could be seen as amounting to an invitation to the Commissioner to revisit a decision scrutinised and endorsed by the Commissioner.

10.55 We do not see this objection as fatal to the recommended scheme. First, the conflict is more apparent than real. In practice, the warrant will have been scrutinised by a Judicial Commissioner; it is entirely possible for that decision to be investigated by another Judicial Commissioner acting in their usual independent capacity without interference by the original parties. Secondly, there may nevertheless be merit in IPCO revisiting the original scrutiny of the warrant since the complaint may reveal new evidence causing it to change its view on the propriety of the warrant. Thirdly, since we recommend that IPCO must report to the ISC on its investigations, there is independent scrutiny of the process that should provide confidence in its rigour.

10.56 In those rare instances where IPCO or the SC is genuinely conflicted, this might weigh in favour of a subsequent public disclosure being afforded protection under Article 10 through the public interest defence that we recommend. However, taken as a whole (ie including the SC), there would be sufficient avenues for reporting concerns that it seems unlikely that every authorised avenue for disclosure would be ineffective. One could, for example, report to the ISC in the alternative.

APPEALS PROCESS

10.57 As the SC would be operating a quasi-judicial function as well as an investigatory function, it would be necessary to allow those with sufficient standing (which should include the original complainant) to appeal the decision of the SC. However, given the sensitive nature of the information the SC will have in its possession – and the fact

that the substance of the complaint will not have been subject to proof in open court – an appeal through the usual channels would not be appropriate.

10.58 We consider that the Investigatory Powers Tribunal (IPT) would be the most appropriate body to hear appeals from the SC, and thus we recommend expanding its jurisdiction to hear these appeals.

10.59 At present, the IPT is an independent court (not part of Her Majesty's Courts and Tribunal Service) that has jurisdiction to hear complaints from those who have been the victims of unlawful interference by public authorities using covert techniques regulated under the Regulation of Investigatory Powers Act 2000 ("RIPA"). The Tribunal also considers complaints about the conduct of MI5, SIS, GCHQ and the UK Intelligence Community more broadly. It is also the appropriate forum to consider infringements of human rights by those agencies. The Tribunal is presided over by a person of high judicial office (currently Lord Justice Singh), and the members include senior members of the professions and judiciary.

10.60 The Tribunal has powers to order and receive evidence, including secret evidence, and to compel the co-operation of public bodies in the conduct of its investigations. It has extensive experience in dealing with sensitive material and has procedures in place to meet its obligations in keeping from disclosure such material, especially as it relates to sensitive operational material from the security and intelligence agencies.

10.61 There are further benefits for appellants that attend to the use of the IPT: it is free of charge, and could provide confidentiality to protect the appellant and the fact that he or she had appealed a decision of the SC (as is the case currently with applicants in the IPT).

10.62 As the IPT is both an investigative and adjudicative body, it has the powers and experience to conduct further investigation should that be necessary. We see no compelling reason for excluding from its appellate function the right to conduct further investigation where it considers it necessary. Given that the appellant is not necessarily in a position to introduce extensive evidence, it would be entirely appropriate for the IPT to exercise its investigative function where it considered it necessary in assessing the evidence provided by the SC.

10.63 However, the appeal should not, in and of itself, be the basis for a second, full investigation. The primary concern of the IPT, as a reviewing tribunal, would be to ensure that the SC has met its obligations under the law.

10.64 The IPT should therefore be concerned to ensure that the SC has conducted an appropriately extensive investigation, having regard to the complexity, urgency and importance of the complaint, sufficient to justify its determination on the outcome, and that such determination was not unreasonable given the findings of the investigation. Therefore, the IPT should be slow to interfere with the SC's evidential findings unless it is apparent, for example, that there were meaningful avenues of investigation that were not explored, or statements that were insufficiently interrogated. As the IPT is both a judicial and an experienced investigative body, such an inquiry falls well within its expertise.

10.65 Of course, were the IPT unable to act expeditiously itself, this would undermine the requirement that the SC act expeditiously. There would therefore have to be clear timeframes or duties of expedition in relation to the appeals process.

10.66 In order to avoid the risk that the appeals system is abused, permission would have to be sought from the IPT who, on receipt of an application, would conduct sufficient enquiries of the SC to determine whether there are grounds to suggest it had not complied with its legal obligations.

10.67 Following an appeal, should the IPT conclude that the SC had fundamentally fallen short of its duty to investigate the claim, then it would be entirely appropriate for the IPT to substitute its own order, if enough evidence is able to be brought before the tribunal to enable it so to do. Alternatively, where it is clear that a significant further investigation will be required, the IPT may remit the case to a different member of the SC (such as a Judicial Commissioner at IPCO).

10.68 Given that complainants will not necessary know on what grounds the SC has reached a determination, it is unlikely that they will be able to form, either specifically or at all, any grounds for appeal. The burden will therefore fall on the IPT to determine the grounds of appeal.

10.69 The Supreme Court have held that the High Court has jurisdiction in reviewing the lawfulness of IPT determinations.[659] Rulings can also be challenged by way of application to the European Court of Human Rights.

10.70 There is also, following section 242 of the Investigatory Powers Act 2016 which amends section 67 of RIPA, a right of appeal from decisions and determinations of the Tribunal on points of law that raise an important point of principle or practice, or if there is some other compelling reason for granting leave to appeal. If permission to appeal is granted, the appeal will be determined by either the Court of Appeal (in England and Wales) or the Court of Session (in Scotland).

THE STATUTORY COMMISSIONER AND ITS RELATION TO THE PUBLIC INTEREST DEFENCE

10.71 The duty of loyalty and discretion owed by public servants, and particularly members of the security and intelligence services (see our discussion in Chapter 9), leads us to conclude that there ought to be a strong presumption that public servants make disclosures about alleged wrongdoing to the SC in preference to public disclosure. By this, we are not denying the public servant the public interest defence if he or she does make an unauthorised disclosure, but the decision not to use the SC when it was available will weigh in the assessment of whether the disclosure was, taken as a whole, in the public interest.

10.72 We discuss the public interest defence in the next chapter. For now, it suffices to say that any assessment of whether a disclosure was in the public interest involves two questions: (i) was the subject matter of the disclosure in the public interest; and, (ii) was the manner of disclosure in the public interest? Such a formulation avoids simplistic appeals to the public interest regardless of the negative consequences,

---

659 *R (on the application of Privacy International) v Investigatory Powers Tribunal and others* [2019] UKSC 22.

where the cure is worse than the disease. For example, someone may have a legitimate concern about evidence that the intelligence services are acting without regard to the mental health of their covert human intelligence sources, but if the public disclosure of that evidence results in the deaths of those same people, the disclosure, viewed as a whole, was not in the public interest.

10.73 We do not consider that members of the public should be compelled to use the SC, albeit that the opportunity should be available to them. As with Crown servants, the availability of the SC will necessarily weigh in any assessment of whether a disclosure made without recourse to the SC was in the public interest. But the lack of a prior duty of discretion necessarily means that it will weigh less heavily against members of the public, including journalists.

10.74 So, while the same public interest defence would be available for both public servants and for members of the public, it will generally be the case that members of the public, including journalists, are afforded slightly greater protection by that defence. We consider that this is in line with Article 10.

INJUNCTIONS AND PRIOR RESTRAINT

10.75 In this section, we consider whether injunctive relief conflicts with the use of the SC and the public interest defence. If the Attorney General sought an injunction upon hearing of a potential disclosure, would this have the effect of prohibiting disclosure regardless of the SC investigation? As will be seen, we do not consider that the use of injunctions fundamentally undermines the disclosure regime we have outlined.

What is an injunction?

10.76 A prohibitory injunction is an order by the court that the defendant refrain from doing a specific act or acts. An example of a prohibited act might include, for these purposes, the criminal disclosure of official data or breach of contractual obligations under an employment contract.

10.77 An injunction can be either interim or perpetual. Perpetual (or ‘final’) injunctions are granted as a remedy for the claimant following a full trial on the merits of the case. Interim injunctions are granted pending a full trial.

10.78 Breaching the terms of the injunction may constitute a contempt of court and may thus be a criminal offence. This means that a defendant – and in some cases a third party – who discloses official data without authorisation could, if there is an injunction in place, be guilty of both the Official Secrets Act offence and of a contempt of court.

10.79 Injunctions are not granted without cause: there is no such thing as an injunction ‘in the air’ without proof by the applicant that their legal rights either have been or are likely to be infringed. So, by way of example, the Attorney General could not ask a

court for a blanket injunction covering all possible future disclosures of official data by any potential defendant.[660]

10.80 Further, any injunction that restrains speech or publication would be subject to stringent scrutiny by the courts. The court is obliged, under Article 10 of the European Convention on Human Rights, to have regard to the defendant's right to freedom of expression. Speech that concerns political opinions, facts, or speaking truths to power will be held in particularly high regard, so interferences in such freedoms will require a similarly high level of justification.[661]

The liability of third parties

10.81 It is important to note that, whilst an injunction binds only the named defendant, third parties are not entitled to act with impunity with respect to the injunction. A third party, even a third party acting entirely independently of the party against whom the order was made, may deliberately frustrate the purpose of the injunction and so be guilty of contempt.[662] It is equally possible that a third party could be found guilty of aiding and abetting the named party's breach of the order.

10.82 The paradigm case was *AG v Punch Ltd*.[663] The magazine *Punch* and its editor, Mr Steen, were found guilty at trial of contempt of court. They had published articles written by David Shayler, the former MI5 officer, who was the subject of an interim injunction prohibiting him from disclosing "any information obtained by him in the course of or by virtue of his employment in and position as a member of the Security Service…" The House of Lords held that the trial judge was correct to hold that both the conduct and the fault elements of the contempt offence had been proved to the requisite high standard.

10.83 Specifically, the House of Lords held that *Punch* and Mr Steen had, by publishing, wilfully frustrated the purpose of the order (although Lord Nicholls of Birkenhead also considered that they could have been found guilty of aiding and abetting Mr Shayler's breach of the order, but the Attorney General had not advanced the appeal on this basis).[664]

The purpose of injunctions

10.84 Interim injunctions and perpetual injunctions serve different purposes. The orders may be worded in a very similar way and thus may have similar effect – prohibiting or mandating certain action pending discharge by the court – but effect and purpose are not synonymous.

---

660 Even the rare injunction *contra mundum*—that is, an injunction 'against the world'—that lacks a named defendant requires that there is a real, extant risk: see *R (Press Association) v Cambridge Crown Court* [2012] EWCA Crim 2434 and *Venables v News Group Newspapers Ltd* [2010] EWHC B18 (QB).

661 See, for example, *Interflora Inc v Marks and Spencer plc* [2014] EWHC 4168 (Ch) and our discussion in paragraph 9.76.

662 *Attorney General v Punch Ltd and another* [2003] 1 AC 1046.

663 *Attorney General v Punch Ltd and another* [2003] 1 AC 1046.

664 *Attorney General v Punch Ltd and another* [2003] 1 AC 1046 at [3].

10.85 A distinction is also to be drawn between the purpose of the injunction and the reasons that may dictate whether it is to be granted or why a party might wish it. The Attorney General's reasons for seeking an injunction may be that it would better protect national security. A court's reason for refusing to grant an injunction may be that it would constitute a disproportionate infringement of the defendant's Article 10 rights. Neither reason reveals, however, what the purpose *in law* of the injunction is.

Perpetual injunctions

10.86 The purpose of the perpetual injunction is the vindication of the rights of the claimant; it recognises interference in the claimant's rights and affirms those rights by explicitly and specifically prohibiting further interference in them. It is granted at the discretion of the court following a full trial. The perpetual injunction is inherently remedial.

10.87 By way of relevant example, let us consider that Officer X intends to disclose confidential official data. The Crown has a proprietary right to that data, the Attorney General has a right to ask the court to assist in enforcement of the law, and, further, the Crown is owed duties of confidentiality by Officer X in respect of that data. If that data is disclosed, it will be an affront to these rights. Of course, the court may or may not grant a perpetual injunction in this case; much will turn on whether, for example, the Crown's rights and interests are trumped by the defendant's own right to freedom of expression. If the court were to grant the perpetual injunction having considered the merits of the claim, it would provide redress to the claimant by restoring or protecting the claimant's rights.

Interim injunctions

10.88 Given that interim injunctions necessarily predate a determination of the merits of the case at trial, their purpose is not remedial. Rather, the interim injunction preserves the status quo pending determination of the merits following a full trial.

10.89 In *AG v Punch* – which concerned an interim injunction – their Lordships considered what was meant by "the purpose of the order". The primary purpose in granting the interim injunction is to ensure the best administration of justice in ensuring "that the court's decision on the claims in the proceedings are not pre-empted".[665] Were the terms of the interim injunction to be contravened, there is then a real risk that the subject-matter of the claim will be defeated or destroyed. Confidential information is a particularly useful example of this.

Injunctions and the use of the SC

10.90 People considering reporting alleged wrongdoing to the SC will have to consider many factors. One will be that the investigation will alert authorities to the existence of a person threatening to publish, and this may prompt the Attorney General to seek an injunction. This would have the effect of taking decisions on public disclosure out of the SC's hands and criminalise any subsequent disclosure as a contempt of court.

10.91 We are alive to the concern, but consider that there are a number of reasonable mitigations.

---

665 *Attorney General v Punch Ltd and another* [2003] 1 AC 1046 at [47].

10.92 First, as noted above, an interim injunction will only be granted where it is likely that someone's rights have been or will be infringed or, in the case of actions brought by the Attorney General, that a crime is likely about to take place. As the disclosure to the SC is, by definition, an authorised disclosure, this will not constitute an infringement of the Crown's rights in that confidential information, nor a crime. To the extent that a disclosure to the SC might signal that there will potentially be an unauthorised disclosure, there would need to be specific evidence to this effect.

10.93 Secondly, and in any event, the court is obliged to have regard to Article 10 and the proportionality of the interference (as discussed above). The more serious the wrongdoing suggested by the disclosure, the higher the level of justification that will be required of the interference. Further, in the case of a disclosure for journalistic, artistic or literary purposes, the court is obliged (under section 12(4)(a)(ii) Human Rights Act 1998) to consider the specific question of whether it is in the public interest for the material to be published.

10.94 Thirdly, depending on how the legislation is drafted, where the SC is investigating a claim in order to make a judgment on public disclosure, it might be acting in a judicial capacity. It would be inappropriate for another court to grant injunctive relief that had the effect of overriding the jurisdiction of the SC in making determinations on disclosure. Even if it is, in all the circumstances, appropriate to grant injunctive relief in order to protect the rights of the Crown pending determination by the SC, the injunction ought to go no further than this.

10.95 If the SC rules that disclosure was not in the public interest, and if the individual were clearly going to make a public disclosure nonetheless, then the Attorney General may well seek injunctive relief. As first law officer of England & Wales, the Attorney General would be acting within his or her jurisdiction – and acting entirely properly – to ask the court for assistance in enforcing obedience with the law. Certainly, there would seem to be nothing improper about seeking injunctive relief pending the outcome of an appeal or judicial review process. However, the court, in granting injunctive relief, would be obliged to consider the public interest. It would need to do so both as a function of section 12(4)(a)(ii) of the Human Rights Act 1998, and because, in determining the merits of the Attorney General's claim, it would need to consider the likely success of the public interest defence at trial. Therefore, it would not be sufficient that the SC had not considered disclosure to be in the public interest: this may be evidence in an assessment of the public interest (and the SC may well be an intervener in any hearing), but the court would not treat that judgment as determinative of its own public interest test. The defendant would therefore be entitled to make submissions on the public interest at this stage.

10.96 A without-notice application would self-evidently not allow the defendant the opportunity to raise public interest arguments him or herself, but this does not mean that the court is able to ignore the public interest question. Indeed, this is itself a judicial process, so injunctive relief is not a process without external checks on executive power.

10.97 First, and in any event, the court must at least be satisfied (having been presented with evidence to this effect) that there were good reasons for not giving notice, and should not consider a without-notice application unless it is clear on the evidence that

there was literally no time to give notice or that giving notice would enable the defendant to take steps to defeat the application (Civil Procedure Rule 25.3.2).

10.98 We consider that it is entirely possible that the applicant will be able to satisfy these criteria: if a defendant is threatening to publish, then the ease of disclosing that information to a wide audience means that the very act of giving notice may render any equitable remedy – such as an injunction – vain.

10.99 However, second, under Practice Direction 25A.5.1(3), interim orders for injunctions without notice must contain a return date for a further hearing at which the defendant can be present. Therefore, injunctions are not a route for overriding the judgment of the SC (or indeed the IPT), nor are they mechanisms for avoiding judicial scrutiny of the public interest. Further, we do not consider that the mere existence of a complaint to the SC would or should be grounds upon which the Attorney General could claim injunctive relief. Even if it becomes clear that a journalist intends to publish material, it is worth reiterating the effect of section 12(4)(a)(ii) of the Human Rights Act 1998, under which the court is obliged to consider the public interest in the publication of journalistic material.

CONCLUSION

10.100 We therefore recommend that a statutory commissioner should perform the following additional functions:

(1) Those who fall within the ambit of the offences under the Official Secrets Act 1989 should be able to approach the SC to report evidence of serious wrongdoing.

(2) The SC would then come under a duty to conduct a timely and effective investigation in order to determine how best to effect redress, which may include passing evidence to appropriate law officers or enforcing redress of its own accord.

(3) We also considered that it would be appropriate in all cases for the SC to make some form of public disclosure, having determined in what manner the results of their investigation should be disclosed.

10.101 On the matter of public disclosure, the SC would have a number of options open to it.

(1) Where the SC's investigation does not uncover wrongdoing, then the disclosure may be limited to a confirmation that a complaint was received and an investigation was undertaken that revealed no wrongdoing. The extent to which the SC chooses to elaborate on the nature of the investigation (which was the relevant agency, for example) or on the nature of the complaint (what was the allegation) will be a matter for it considering the public interests in transparency and national security.

(2) If the SC's investigation does reveal wrongdoing, then the SC could be tasked with pursuing a number of options for disclosure. These include, but would not be limited to, one or more of the following:

(a) authorise the complainant to make disclosure in full or redacted form;

(b) disclose the original material on its own or in conjunction with material uncovered from the investigation, each in full or redacted form;

(c) submit a dossier of evidence to the appropriate prosecutorial body (if the wrongdoing amounted to a crime); and

(d) make a public statement that wrongdoing was uncovered in the course of an investigation and that a full report will be made public in due course.

10.102 The precise terms of operation of the SC are a matter for government and the relevant powers and duties bestowed on the SC. The option the SC chooses from whatever range it is granted will, in each case, be determined by its assessment of the public interest. We consider that there should be guidelines on the content of the public interest test, in order to aid consistency and transparency, though we have not consulted on this.

10.103 The SC should come under an obligation to report to the Prime Minister. Further, requiring the SC to make similar reports of its investigations in this respect to the Intelligence and Security Committee of Parliament would add a further level of transparency and oversight given the cross-party nature of the parliamentary committees.

10.104 In any event, the SC will be required to publish generalised statistics of its investigations, as it currently does in respect of its other responsibilities.

10.105 There should be an automatic right of appeal by the complainant against decisions of the SC. The jurisdiction of the Investigatory Powers Tribunal should be expanded such that it can hear appeals against decisions of the SC.

10.106 The jurisdiction of the SC should not be overridden by the use of injunctions, even though interim injunctions *may* be appropriate while an investigation is ongoing.

10.107 There may be rare instances where, because of urgency or conflicts of interest, it is not in the public interest to consult the SC prior to a public disclosure, but we caution against simplistic application of these exceptions.

Recommendation 32.

10.108 An independent, statutory commissioner should be established with the purpose of receiving and investigating allegations of wrongdoing or criminality where otherwise the disclosure of those concerns would constitute an offence under the Official Secrets Act 1989.

10.109 That commissioner would have to constitute an effective investigative mechanism: it would therefore have not only to be independent, but also be able to act expeditiously and have the legal authority to compel cooperation with its investigations.

10.110 There should be a right of appeal by the complainant against decisions of the statutory commissioner. The jurisdiction of the Investigatory Powers Tribunal should be expanded such that it can hear appeals against decisions of the statutory commissioner.

Chapter 11: Public Interest Defence

INTRODUCTION

11.1 Having recommended the first limb of our public interest disclosure model – the statutory commissioner – we move now to consider the second: the public interest defence, and the general form a public interest defence ought to take.

11.2 A public interest defence would allow a defendant to justify their unauthorised disclosure on the broad basis that disclosure of information was in the public interest. In the event that the jury agreed, the defendant would not be guilty of the offence.

Our Consultation Paper

11.3 The Official Secrets Act 1989 ("OSA 1989") does not contain a public interest defence. Our Consultation Paper examined whether one should be introduced. Having considered the approaches in other jurisdictions and the potential benefits and costs more generally, we provisionally concluded that no public interest defence should be introduced. We arrived at this provisional conclusion based on our assessment that the disadvantages of introducing a public interest defence outweighed the advantages. This was, however, only a provisional conclusion and we welcomed consultees' views on whether they agreed with it or not. This proved to be one of the most controversial parts of the Consultation Paper.

11.4 We received many detailed and considered responses that discussed this question. Many consultees argued robustly in favour of introducing a broadly formulated public interest defence. On the other hand, it has been the firmly and consistently held view of successive Governments that a public interest defence is not desirable in the context of official secrets legislation. During the passage of the Official Secrets Bill, which became the OSA 1989, a number of amendments sought to insert a public interest defence into the Bill, but they were all rejected.

11.5 Our engagement with stakeholders did not end with the written responses we received. During the three-month consultation period and in the time since it closed, we have continued to meet and engage with consultees, including representatives from the media, academics, representatives from NGOs, practitioners and representatives from various government departments. As noted in Chapter 8, consultees provided extensive feedback on the concerns we had raised in the Consultation Paper. We are grateful for both the quality and extent of this input, which has enabled us to examine further the provisional conclusion we reached in our Consultation Paper.

Our recommendation for a public interest defence

11.6 In this chapter, we recommend that a public interest defence be available for offences under section 1-6 of the Official Secrets Act 1989 (which, by implication, means that those who could avail themselves of the defence would include Crown servants and journalists). We address a number of questions regarding the form of the defence, including the burden of proof and the elements of the defence that must be satisfied,

and therefore suggest a form of defence in skeletal form. For example, it is important to bear in mind that any assessment of whether the disclosure was in the public interest will necessarily have to take account of whether the chosen manner of disclosure risked more damage than was necessary: therefore, a Crown servant relying on the defence would be required to demonstrate why the authorised methods of disclosure (such as the Statutory Commissioner ("SC") proposed in the preceding chapter) did not adequately serve the public interest.

11.7 As we did not propose a public interest defence in our Consultation Paper, we did not consult on the details of any public interest defence. Therefore, we do not consider that it would be appropriate for us to propose a detailed draft of a defence. In this chapter, we consider certain attributes that any defence would require, and we note existing defences in other jurisdictions, but the detail of any such defence in the UK will necessarily be a matter to be taken forward by the Government.

11.8 In light of the above, there are specific matters that we will not address. These include:

(1) the scope of application of the defence, given the existence of authorised methods of disclosure such as the SC (ie the range of circumstances in which it is possible that the SC etc will *not* constitute an effective investigative mechanism); and

(2) the factors that courts and juries must take into account when deciding whether the defence is made out (which includes the factors determining the public interest).

We, unlike the Government, do not have the evidence necessary to draft with confidence on these matters.

WHY IS A PUBLIC INTEREST DEFENCE DESIRABLE?

11.9 In the preceding chapters, we have sought to provide a justification for our proposed public interest disclosure model, consisting of a statutory commissioner fortified by a public interest defence. It will be recalled that we consider that such a model helps to ensure that our official secrets regime strikes a fair balance between the public interest in national security (and all that such an interest entails) and the public interest in transparent and accountable government. The model also provides adequate protection to Article 10 rights under the European Convention on Human Rights.

11.10 As we noted in Chapter 9, a public interest defence is not mandated under the European Convention on Human Rights. Compliance with Article 10 (freedom of expression) requires that there is a proportionate relationship between an interference in freedom of expression and the aim thereby pursued. The margin of appreciation afforded to states in protecting official data must not be used to mask wrongdoing (howsoever defined). So, whilst some interferences in freedom of expression, by prosecuting disclosures, will be legitimate (for example, where they are in the interests of national security), an interference will not be legitimate if its purposes is merely the suppression of evidence of wrongdoing, and so will fall outside the state's margin of appreciation. Interferences are more likely to be legitimate to the extent that they do

not frustrate the purpose of investigating and remedying this wrongdoing. The question of whether a public interest defence was necessary for compliance with Article 10 ECHR will therefore be fact-dependent. A defence is unlikely to be necessary so long as, in the case in question, there existed effective investigative mechanisms.

11.11 We noted that journalists may be afforded greater protection in exercising their right to freedom of expression on the basis that, unlike public servants, they did not owe a prior duty of loyalty, reserve and discretion.[666] This will weigh in the balance when assessing proportionality. However, again, this does not necessitate a public interest defence in and of itself.

11.12 Given the fact-dependence of any judgment on compliance, general pronouncements that a state's regime of data protection is "Article 10 compliant" or otherwise are somewhat misdirected, save perhaps for extreme cases. It is, of course, possible to envisage situations where a public interest defence might be necessary for compliance, but that mere fact would not automatically mean that any state lacking such a defence was non-compliant. The interferences of that state may have been – and may continue to be – entirely proportionate on the facts of cases before the courts.

11.13 However, even though the ECHR does not mandate a public interest defence in all cases, there may be situations where the availability of a public interest defence would ensure compliance with Article 10 when no other mechanism could. Investigative mechanisms that are normally entirely effective may, on a given case, be rendered ineffective. This, as may be recalled from Chapter 9, was the situation in *Bucur and Toma v Romania*.[667] In that case, the appropriate method for employees to raise concerns or seek redress of wrongdoing was to make a report to their superiors. However, the alleged wrongdoing concerned the employees' superiors themselves, and thus the court doubted (not unreasonably, in our view) the effectiveness of any report that the applicants could have made.[668] In light of this, the court considered that a public disclosure should be afforded protection under Article 10.[669]

11.14 The introduction of a public interest defence would therefore increase the likelihood that the UK would be Article 10 compliant in all situations. This is because it provides a backstop in the event that the mechanisms for investigation and redress are rendered ineffective.

11.15 On this basis, there would be a role for a public interest defence in the United Kingdom. Whilst the statutory commissioner model outlined in the previous chapter – along with the many internal avenues for reporting concerns (the Intelligence and Security Committee, staff counsellors, the Attorney General, the Director of Public Prosecutions etc) – will ensure that an effective investigative mechanism exists in most situations, it is at least conceivable that these may be rendered ineffective

---

666 See, for example, 9.74 above.

667 *Bucur and Toma v Romania (40238/02)* [2013] ECHR 14.

668 *Bucur and Toma v Romania (40238/02)* [2013] ECHR 14 at [97].

669 *Bucur and Toma v Romania (40238/02)* [2013] ECHR 14 at [100].

(a possibility we consider in Chapter 10). The availability of a public interest defence in those situations would ensure that the UK has afforded sufficient protection to the Article 10 rights of those who make unauthorised disclosures that reveal or prevent wrongdoing.

11.16 If a concern was raised about the activities of Government and law enforcement, and the SC was unable to make effective investigation of this (because of, for example, time constraints), it may well be the case that compliance with Article 10 could only be achieved by a public interest defence.

WHAT IS DISTINCTIVE ABOUT A PUBLIC INTEREST DEFENCE?

11.17 A true public interest defence is a justification of conduct and not an excuse for it. It is a finding by the court that the disclosure was in fact in the public interest, not merely that the person making the unauthorised disclosure believed it to be in the public interest. Such a defence would be available even if the motive of the defendant were entirely one of malice or self-interest. For similar reasons, it would be no defence that the defendant *believed* that he or she was acting in the public interest but, in fact, was not.

11.18 The courts have long been wary of allowing people to subvert the criminal law on the basis of expediency, not least because this would "import an undue subjectivity into the criminal law" and because "it would invite the courts to second-guess the legislature and to assess the relative merits of social policies underlying criminal prohibitions."[670] Of course, a statutory public interest defence mitigates these concerns to some degree: the legislature would have bestowed upon courts the authority to assess the merits of the conduct, but within a narrow scope (namely where necessary in the public interest).

11.19 Nonetheless, defences that rely upon concepts such as public good and public interest are unusual in English criminal law. Juries are asked to balance two concepts without knowing how much weight they should attribute to each. For the vast majority of defences in criminal law, the jury is not required to make a value judgement about the merits for society of the defendant's conduct. Their inquiry is confined to considering narrowly defined issues, such as, in the case of self-defence for example, whether the defendant genuinely believed it was reasonable or necessary for him to use force to defend himself and the amount of force was reasonable in those circumstances. The jury's conclusion on this issue will be informed by their assessment of the defendant's explanation of what took place and their collective experience of human nature. In the context of a public interest defence, the jury are being asked to balance competing interests which are likely to be far outside their realm of experience.

11.20 There are, however, defences in the criminal law of England and Wales that are similar to public interest defences. For example, the "public good" defences found in obscenity law allow certain justifications for the publication of obscene material.[671]

---

670 *Perka et al v The Queen* [1984] 2 SCR 232, 248. See also *Southwark LBC v Williams* [1971] Ch 734, 746 (Edmund Davies LJ); *R v Dudley and Stevens* (1884) 14 QBD 273 (DC).

671 See J Jaconelli, 'Defences to Speech Crimes' (2007) 1 *European Human Rights Law Review* 27.

Section 4(1) of the Obscene Publications Act 1959, for example, states that a person who publishes an obscene article contrary to section 2 of that Act shall not be convicted if publication of the article is "justified as being for the public good on the grounds that it is in the interests of science, literature, art or learning, or of other objects of general concern". Both the prosecution and the defence are entitled to call expert witnesses to establish whether the publication may be justified as being for the public good.[672] A "public good" defence in obscenity law does not amount to a denial of harm. The article remains obscene, but its obscenity is justified on the grounds that its publication is in the "public good". This is the same role as is played by the concept of public interest in the context of unauthorised disclosure offences.

11.21 In our Consultation Paper, we examined the few examples of true public interest defences in the criminal law of England and Wales. We paid particular attention to the defence that was then contained in section 55 of the Data Protection Act 1998. We also examined the very narrow public interest defences set out in section 20 of the Commissioners for Revenue and Customs Act 2005 and section 3 of the Agricultural Statistics Act 1979. We concluded that none of these examples offered a workable model for a public interest defence that could be pleaded in respect of the offences contained in the Official Secrets Act 1989.

A TRUE PUBLIC INTEREST DEFENCE

11.22 It is our view that any such defence in the OSA 1989 would need to be a true public interest defence. It should only be a defence if the disclosure was in fact in the public interest. There are two reasons for concluding that it should not be sufficient (or even necessary) that the defendant believed the disclosure was in the public interest.

11.23 First, even if a defendant's ostensibly noble ambition may cause some to question the extent of his or her moral culpability, it does little to mitigate the basis of criminal culpability. The aim pursued by the Government in restricting disclosures is to protect national security. This is a legitimate aim under the ECHR and there is a clear public interest in national security – in the faith we place in and authority we bestow upon governments to ensure our safety and security. The Government also has obligations to protect the lives of those who serve it. Both of these legitimate aims can be frustrated by an unauthorised disclosure (whoever makes the disclosure), and potentially to devastating effect. Indeed, currently under all but the section 1(1) offences (that apply to members of the security and intelligence services), it will be a matter of proof *beyond reasonable doubt* that the defendant will have caused or was likely to have caused damage by their disclosure. Even under our recommended reforms, this will still be the case for sections 5 and 6. It will be cold comfort to know that the defendant happened to think – however reasonably – that they were acting in the public interest albeit that, in fact, they were not.

11.24 Secondly, an unauthorised disclosure by a Crown servant carries with it inevitably an element of recklessness as to the damage that may be wrought by an unauthorised disclosure. The defendant will have or ought reasonably to have foreseen this risk (albeit that some of the offences are offences of strict liability, so do not require this element of recklessness or foreseeability to be proven for the purposes of the

672 Section 4(2) Obscene Publications Act 1959.

offence). Ought the defendant's belief that his or her conduct in disclosing was in the public interest be enough to negative the culpable state of mind prescribed in the offences? Such a judgement by the defendant would involve him or her assuming the risk that the disclosure may cause more damage than he or she could have foreseen. This element of recklessness, however noble the motive, ought not to be rewarded in the criminal courts (or at least not without some further proof that it was justified).

11.25 For the avoidance of doubt, motive is to be distinguished from the fault element of an offence. The fault elements are those elements that the defendant must be proven to have intended to be guilty of the crime. So, in the case of murder, the defendant must have intended to kill or cause serious harm. By contrast, motive is the *reason* that the defendant committed the crime. So, staying with the example of murder, the murderer intended to kill the victim *in order to prevent him disclosing the details of a crime*. There may be instances where good intention is enough to negative the finding of the fault element – perhaps the murderer did not intend to kill at all, but only did some well-meaning act that, through no intention of the defendant, resulted in death. However, where the fault element of the crime is met, it will not be sufficient to show that the motive was noble.

IS IT NECESSARY TO HAVE DIFFERENT DEFENCES FOR DIFFERENT CATEGORIES OF DEFENDANT?

11.26 Given that a public interest disclosure serves as a backstop that ensures compliance with Article 10 where other mechanisms of redress are ineffective, there is no reason that the public interest defence should not be available to anyone charged with an offence under the Official Secrets Act 1989, whether or not the offence is one of strict liability. Thus, it would be reasonable to expect it to apply to notified individuals, intelligence officers, Crown Servants and journalists alike.

11.27 As we noted in Chapter 10, there may be different Article 10 considerations that would apply to Crown Servants and journalists that affect the operation of the defence, but their differing roles and professional obligations do not, in and of themselves, necessitate a different defence.

BURDEN OF PROOF

11.28 In broad terms, there are two forms that the public interest defence could take. Both involve a form of burden of proof on the defendant, which is known as a reverse burden of proof:

(1) the defendant must raise an issue of public interest sufficient to require the prosecution to disprove it as part of the burden of proof resting on the prosecution (an "evidential burden"); or

(2) the defendant must show, on the balance of probabilities, that the disclosure was in the public interest (a "legal burden" or "persuasive burden").

11.29 The distinction concerns the burden of proof and the party on whom it rests. In the former, the burden of proof remains with the prosecution, and they must prove beyond reasonable doubt that the disclosure was not in the public interest. The latter requires

that the defendant prove that the disclosure was, more likely than not, in the public interest.

11.30 There are numerous examples of reverse legal burdens of proof and rebuttable presumptions in English law. Some examples include:

(1) section 40 of the Health and Safety at Work Act 1974, which states "it shall be for the accused to prove… that it was not practicable or not reasonably practicable to do more than was in fact done to satisfy the duty or requirement…";

(2) section 101 of the Magistrates' Courts Act 1980, which states "Where the defendant to an information or complaint relies for his defence on any exception, exemption, proviso, excuse or qualification… the burden of proving the exception, exemption, proviso, excuse or qualification shall be on him…";

(3) section 139(4) of the Criminal Justice Act 1988, which provides that "It shall be a defence for a person charged with [having a bladed or pointed article in a public place] to prove that he had good reason or lawful authority for having the article with him in a public place"; and

(4) section 4 of the Homicide Act 1957, which provides that it will be manslaughter and not murder if, under subsection (2), the defence "prove that the person charged was acting in pursuance of a suicide pact between him and the other."

11.31 It is our view that the second formulation, the legal burden, is preferable. First, placing the burden of proof on the prosecution might make impossible demands of the prosecution, rendering the defence a *fait accompli* – its success might become a virtual certainty at the point that it is raised. Consider the following example:

> Defendant, D, has disclosed a document in breach of the 1989 Act. The implication of this document is that the UK special forces have been engaged in illegal conduct, owing to a reference to "special forces operating in Ruritania". D argues that there is therefore a public interest in publishing the document. However, the inference sought to be drawn from the document, and thus the basis of the public interest in publishing it, is entirely incorrect: despite the apparent implication of the document, there has been no illegal conduct as the reference was not to *UK* special forces.

11.32 If the defendant bears only an evidential burden (to raise the public interest defence), but the prosecution bears the legal burden to disprove it, the prosecution in this example would be required to prove a genuine negative – that their special forces were not operating in Ruritania – beyond reasonable doubt. Anything less than this would leave a reasonable doubt as to the defendant's guilt: a jury may not be sure that disclosure was in the public interest, but they cannot be absolutely sure that it was not. This would be an unrealistically high bar. Further, it is not as if the disclosure scenario described above is sufficiently atypical or eccentric to render these concerns inconsequential.

11.33 Secondly, any attempt to meet this burden of proof by the prosecution would require extensive disclosure of information. We have already expressed significant misgivings in this respect in relation to the damage requirement. To require further disclosure to

prove a further element (that will not necessarily align evidentially with the damage requirement) would seem to be compounding the problem. We understand the criticism of some consultees that evidence was not provided to support the assertion that prosecutions might be avoided on the basis of the evidential demands of the damage requirement, and certainly we cannot adduce evidence of a defence that does not yet exist. However, whilst we follow this argument, we do not agree that this materially weakens our concerns. It requires no special insight or criminal law expertise to suppose that a burden of proof requires evidence to be put before the court, and that the evidence may be of a nature whose disclosure would compound damage or be in conflict with the public interest (especially where the disclosure related to highly sensitive information).

11.34 It is also worth emphasising that defendants will not have to prove the public interest defence beyond reasonable doubt. Their burden of proof is significantly lower: they need merely prove that it was more likely than not that the disclosure was in the public interest (and defences such as these, based on the balance of probabilities, are found in the criminal law as noted above, at 11.30). If the document suggests real wrongdoing and its disclosure has or might prompt an investigation then, whether or not it turns out to be true, there is a plausible argument that its disclosure was likely to be in the public interest. Such a determination would obviously be intensely fact-dependent, but it is important to note that such a defence would not necessarily require the defendant to prove the existence of certain facts (whereas the alternative formulation of the defence would require the prosecution to prove facts or the lack thereof).

Compliance with Article 6(2)

11.35 In recommending a reverse burden of proof, regard must be had to the presumption of innocence under Article 6(2) of the European Convention on Human Rights, because the facts (as least as they relate to the public interest) are presumed against the defendant unless he or she can prove otherwise. However, the European Court of Human Rights recognises certain departures where it is necessary. The interference must be no more than is "reasonably proportionate to the legitimate aim sought to be achieved."[673] As David Hamer writes in his article on the presumption of innocence and reverse burdens, "a balance is sought between the defendant's right not to be wrongly convicted and the community's broader interest in law enforcement."[674] The ECtHR held in *Salabiaku v France* that:

> Article 6(2) does not therefore regard presumptions of fact or of law provided for in the criminal law with indifference. It requires States to confine them within reasonable limits which take into account the importance of what is at stake and maintain the rights of the defence...[675]

---

673 *Janosevic v Sweden (34619/97)* (2004) 38 EHRR 473 at [101].

674 D Hamer, 'The Presumption of Innocence and Reverse Burdens: A Balancing Act' (2007) 66 The Cambridge Law Journal 142, 147.

675 *Salabiaku v France (10519/83)* [1988] ECHR 19, (1988) 13 EHRR 379 at [28].

11.36 Reverse legal burdens are certainly not unusual in domestic law, albeit they are perhaps not commonplace, and they have been considered numerous times by the appellate courts under Article 6(2).[676]

11.37 The House of Lords considered the matter directly in *R v Johnstone*.[677] The case concerned prosecution under section 92 of the Trade Marks Act 1994. Under section 92(5) of the Act, "it is a defence for a person charge with an offence… *to show that he believed* on reasonable grounds that the use of the sign… was not an infringement of the registered trade mark" (emphasis added). The House of Lords were unanimous in holding that the words "to show" placed a clear legal burden on the defendant. The question that Lord Nicholls of Birkenhead considered was whether this legal burden was compliant with Article 6(2).

11.38 Lord Nicholls cautioned that it must be remembered that "if an accused is required to prove a fact on the balance of probability to avoid conviction, this permits a conviction in spite of the fact-finding tribunal having a reasonable doubt as to the guilt of the accused."[678] His Lordship noted that "a reasonable balance has to be held between the public interest and the interests of the individual… It is for the state to show that the balance held in the legislation is reasonable. The derogation from the presumption of innocence requires justification."[679]

11.39 Lord Nicholls therefore explained that the proportionality test was essentially whether "the public interest will be prejudiced to an extent which justifies placing a persuasive [legal] burden on the accused. The more serious the punishment which may flow from conviction, the more compelling must be the reasons."[680] Lord Nicholls held that the reverse burden of proof in that case was justified partly on the basis of the evidential difficulty that would have faced the prosecution in proving dishonesty.[681] These were non-binding opinions by Lord Nicholls, but were cited with approval in *Sheldrake v DPP* by Lord Bingham of Cornhill.[682]

11.40 The Court of Appeal in *R v Webster* also considered that a reverse legal burden of proof would be justified where it was clear that the prosecution would otherwise face insuperable evidential obstacles in many cases.[683]

---

676 See, for example, the House of Lords' opinions in *Lambert* [2001] UKHL 37, [2002] 2 AC 545; *Johnstone* [2003] UKHL 28, [2003] 1 WLR 1736; and *Sheldrake and Others* [2004] UKHL 43, [2004] 3 WLR 976.

677 *R v Johnstone* [2003] UKHL 28, [2003] 1 WLR 1736, [2003] All ER 884.

678 *R v Johnstone* [2003] UKHL 28, [2003] 1 WLR 1736, [2003] All ER 884 at [50].

679 *R v Johnstone* [2003] UKHL 28, [2003] 1 WLR 1736, [2003] All ER 884 at [48].

680 *R v Johnstone* [2003] UKHL 28, [2003] 1 WLR 1736, [2003] All ER 884 at [50].

681 *R v Johnstone* [2003] UKHL 28, [2003] 1 WLR 1736, [2003] All ER 884 at [52]-[53].

682 *Sheldrake v Director of Public Prosecutions* [2004] UKHL 43, [2004] 3 WLR 976 at [33].

683 *R v Webster* [2010] EWCA Crim 2819, [2011] 1 Cr App Rep 16 at [22] (Pitchford LJ). It is worth noting, however, that the court actually found that the reverse burden in that case was not compliant with Article 6(2) because the legal landscape had changed such that those evidential obstacles were generally no longer insuperable.

11.41 We consider that, whilst the reverse burden of proof in the public interest defence would constitute an interference in Article 6(2), the interference is nonetheless proportionate to the legitimate aim pursued.

11.42 First, we have noted above the evidential difficulties that the prosecution will face in many cases. These evidential difficulties will include difficulties borne of having to prove the non-existence of certain events and those borne of the need to disclose further confidential information, further damaging the very aim they have sought to protect.

11.43 Second, most offences under the 1989 Act require proof of damage or proof of likely damage. The prosecution will have discharged this burden *beyond reasonable doubt* in proving the elements of the offence. There is therefore a real public interest at stake, which will weigh in the balance against the interests of the individual. Whilst damage is not an element of the section 1(1) offence, the public interest lies in the confidence the public should have "in the services' ability and willingness to carry out their essentially secret duties effectively and loyally".[684] Not only do members of the security and intelligence services know that their work "carries with it an inescapable duty of secrecy", but also their disclosures "carry a credibility which the disclosure of the same information by any other person does not".[685]

11.44 Third, and related to the second reason, it is relevant that this interference relates to an element of the defence rather than an element of the offence. The burden of proof remains on the prosecution in proving the essential elements of the offence. Courts have long held that, where an interference relates to an exception rather than to the essential elements of the offence, that interference is more likely to be compatible with Article 6(2).[686] The interference does not require the defendant to prove that he is innocent of a crime – there is not a presumption of guilt here (and so we might distinguish the comments of Lord Nicholls in this respect) – but, rather, the defendant is being asked to prove that, if he is guilty of the crime, that conduct was nonetheless in the public interest.

11.45 We have noted in our chapter on Article 10 that these cases are intensely fact-dependant, and so we cannot make a general rule concerning compliance with Article 6. However, we are comfortable that a reverse burden of proof is not precluded by Article 6 in the circumstances we have described and similar circumstances.

PUBLIC INTEREST AND THE METHOD OF DISCLOSURE

11.46 We consider that there is a distinction to be drawn between the public interest in the contents of the document and the public interest in the manner of disclosure. This makes explicit what is implicit in any consideration of whether a disclosure was in the public interest.

11.47 Consider the following example. A disclosure may reveal potential wrongdoing in the security services. The evidence is sufficiently credible to warrant an investigation, and

---

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

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

686 *Attorney-General of Hong Kong v Lee Kwong-Kut* [1993] AC 951, 969H.

thus we would conclude that some disclosure was in the public interest. However, this disclosure is made to the public via social media, rather than to the statutory commissioner whose job it is to investigate these concerns. The result is that a number of legal operations have to be aborted and an officer relocated. Whilst the subject matter of the disclosure is probably in the public interest, the manner of disclosure clearly is not: there are alternative mechanisms that could be used that would have achieved the same or substantially the same positive outcome but with none of the negative outcomes.

11.48 The other reason that it may be in the public interest to make an authorised disclosure to, say, the IPCO rather than direct to the press is because IPCO is far better placed to conduct an inquiry, and may well be able to do so at very short notice. IPCO has a track-record of timely and effective audit of investigatory powers with genuine expertise across a range of services. The mere fact that the cloak of confidentiality has been lifted by the media does not guarantee timely and effective investigation.

11.49 Some may argue that IPCO or the SC would not have been well-placed to investigate on a given set of facts, and that the press was the only effective route for disclosure: if that is the case, then the defendant would be able to advance this argument in court before a jury. This line of reasoning is in line with the Article 10 jurisprudence as we discuss extensively in Chapter 9 concerning effective investigative mechanisms.

11.50 A public interest assessment of the manner or method of disclosure is what gives effect to (amongst many other considerations) the different legal positions of public servants and civilians with respect to Article 10. There is a public interest in public servants' duty of loyalty that has been recognised in ECHR case law. It is clear from that case law that this public interest is not to be ignored completely merely because the subject matter of a disclosure happens also to be in the public interest. Conversely, there is a public interest in, say, a journalist holding government to account.

11.51 What this means in practice is that a journalist who disclosed information may be able to establish a public interest defence whereas a public servant who disclosed that same information – perhaps to a journalist – may not. This position is justified under ECHR case law and reflects the fact that the "public interest" is determined by various factors. However, we do see that this result may be regarded as politically disagreeable by some. Parliament could, of course, choose to legislate in such a way as to avoid this difference; just as the public servant's duty of loyalty provides a sound reason for maintaining the distinction for the purposes of the public interest defence, there may be other political reasons for broadening the scope of public servants' Article 10 rights to match those of civilians. Nonetheless, that is a matter for Parliament; it is not a question for us.

ALTERNATIVE MODELS

11.52 We recommend that the public interest defence to be applicable in the 1989 Act should be a true defence, as described above. We consider that this framework best ensures Article 10 compliance without acting as a barrier to prosecution of genuinely criminal activity. It will need to be further developed. It provides the structure for the decision maker on how to approach whether something was in the public interest.

What is necessary is for the relevant statute to provide further details of which factors the decision maker is to have regard to.

11.53 Whilst we consider a public interest defence to be necessary to ensure compliance with Article 10 in situations where the statutory commissioner will not constitute an effective investigative mechanism, we recognise that there are a range of ways in which a public interest defence can be drafted. It would be for government to select an appropriate form for the defence to take.

A subject-matter approach

Defining "public interest" by reference to a list of factors

11.54 English PEN / Index on Censorship / Journalists Without Borders described a form of public interest defence in terms of the "subject matter approach". In this model, key areas are identified where it would be considered uncontroversial that a disclosure would be in the public interest. English PEN / Index on Censorship / Journalists Without Borders argued that:

> So long as the areas of subject matter are selected with care, this approach to protecting the public interest avoids any theoretical difficulty entailed in defining the public interest in a general sense. Responding to the concerns raised in the Consultation Paper, a public interest defence for the disclosure of official data which was structured in this manner – i.e. as a defence made out where the information disclosed demonstrated criminal or other unlawful conduct – would neither give rise to unworkable uncertainty nor provide cover for partisan political activities.

11.55 Such an approach is taken in section 41(2)(k) of the Digital Economy Act 2017. Section 41(1) of the Digital Economy Act 2017 prohibits the unauthorised disclosure of personal information and is reinforced by a criminal offence. Section 41(2)(k) provides:

> Subsection (1) does not apply to a disclosure –
>
> …
>
> (k) which is made for the purposes of –
>
> (i) preventing serious physical harm to a person,
>
> (ii) preventing loss of human life,
>
> (iii) safeguarding vulnerable adults and children,
>
> (iv) responding to an emergency, or
>
> (v) protecting national security.

11.56 By listing a range of factors, this approach provides greater certainty to the person who is contemplating disclosing information contrary to the criminal law. If a prosecution follows, it also provides the jury with guidance and provides a common point of reference upon which the issues in the trial can be focused. For example, the defendant may justify his or her unauthorised disclosure on the basis that it was made

for the purpose of preventing loss of human life. The prosecution will seek to argue that it was made for some other purpose that is not included in section 41(2)(k).

11.57 We are not suggesting that the list of factors contained in section 41(2)(k) of the Digital Economy Act 2017 should be adopted wholesale in the context of official secrets, even within the framework we have set out. Careful consideration would need to be given to those factors that might justify disclosing information without lawful authority in the official secrets context. Ultimately it would be a matter for Parliament to determine what factors ought to be included in any list, with input from the relevant stakeholders, should this be considered a viable model in future.

11.58 English PEN / Index on Censorship / Journalists Without Borders pointed out that there are limitations with a subject-matter approach to the defence. For example, it may not extend to circumstances where official secrets may be concerned with conduct which is at the edge of existing technological knowledge and existing legal frameworks, and to which Parliament has not yet turned its attention. A definition of public interest which relies upon demonstrating a breach of existing law, while useful, is likely to be of insufficient scope to address the full range of information, disclosure of which would be in the public interest. One possible solution to this problem would be to define the list of factors in a sufficiently broad and open-textured fashion, as we discuss above.

A list of factors specifying what *cannot* be considered to be in the public interest

11.59 A further option is to combine both models. It would be possible to specify the types of disclosure that are not in the public interest and combine this with a list of factors which are relevant to whether the disclosure was in the public interest. This model would have the benefit of providing certainty both for the person who is contemplating making an unauthorised disclosure and, ultimately, for the jury.

A broader, two-fold approach

11.60 As English PEN / Index on Censorship / Journalists Without Border explained, a further approach that could be adopted in the domestic context is to render disclosure lawful not only by reference to subject matter (which serves as proxy for the public interest), but also by reference to the public interest itself (subject to certain appropriate preconditions). The approach taken in Canadian law, in section 15 of the Security of Information Act 2001 (as amended), serves to illustrate this model.

11.61 The Security of Information Act 2001 makes it a criminal offence for any person permanently bound to secrecy to communicate or confirm "special operational information". In our Consultation Paper, we noted that such an individual may not commit an offence if his or her purpose was to reveal that a criminal offence 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.[687] As we discussed in our Consultation Paper, section 15 of the Act provides that a person is not guilty of an offence "if the person establishes that he or she acted

[687] Security of Information Act 2001, s 15.

in the public interest". Acting in the public interest, for the purposes of this test, has two elements.

11.62 The first element relates to the subject matter of the disclosed information. The disclosure must relate to "an offence under an Act of Parliament that [the person] 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". This, in effect, limits the application of the public interest defence to a fairly narrow range of potential disclosures. This avoids the risk of "opening of the floodgates" to unauthorised disclosures, but nevertheless encourages accountability of public officials. It also provides legal certainty, at least in the first limb of the test, as to when a disclosure may have a defence. However, it removes from the scope of the defence any other type of disclosure. If Parliament were to implement this model, careful thought would need to be given to how the defence could be restricted to ensure that this narrowing would be proportionate and compatible with Article 10.

11.63 The second element requires the public interest in the disclosure to outweigh the public interest in non-disclosure. Section 15(4)(a) – (g) of the Security of Information Act lists a number of factors that are relevant when the court is conducting this evaluation:

(1) whether the extent of the disclosure is no more than is reasonably necessary to disclose the alleged offence or prevent the commission or continuation of the alleged offence, as the case may be;

(2) the seriousness of the alleged offence;

(3) whether the person resorted to other reasonably accessible alternatives before making the disclosure and, in doing so, whether the person complied with the relevant guidelines, policies, or laws that applied to that person;

(4) whether the person had reasonable grounds to believe that the disclosure would be in the public interest;

(5) the public interest intended to be served by the disclosure;

(6) the extent of the harm or risk of harm created by the disclosure;

(7) the existence of exigent circumstances justifying the disclosure.

11.64 These factors must be weighed when the court is considering whether the defendant's disclosure was in the public interest. This guides judicial interpretation as to what constitutes public interest and how competing interests should be balanced, while also ensuring that there is sufficient flexibility to deal with the individual factual circumstances of each case. For example, the disclosure of a crime that has been committed by a Government official may also risk disrupting pending investigations of further crime. In such a case, the court would use the factors outlined above to consider whether the public interest in the completion of the pending investigation outweighs the public interest of the people being informed of wrongdoings by their Government.

11.65 The public interest defence contained in the "Canadian model" above therefore has three elements that must be satisfied before the defendant will be acquitted:

(1) the defendant acted with the purpose of disclosing an offence which he or she reasonably believed has been, was being, or was about to be committed by another person in the purported performance of that person's duties and functions for, or on or behalf of, the Government of Canada;

(2) the public interest in disclosure outweighed the public interest in non-disclosure; and

(3) the defendant followed the applicable internal process before making the disclosure.

11.66 The defendant can only rely upon the public interest defence if he or she followed the process set out in the Act.[688] The defendant must have brought the matter to the attention of the relevant organisation's deputy head or the deputy Attorney General of Canada and, if no response is received within a reasonable time, to the attention of the Communications Security Establishment Commissioner[689] or the Security Intelligence Review Committee.[690] Only if there is no response from the Communications Security Establishment Commissioner or the Security Intelligence Review Committee within a reasonable time can the defendant invoke the public interest defence should he or she make a public disclosure.[691]

A public interest defence for journalists

11.67 There are examples in existing statutes of public interest defences for those engaged in journalistic activity. Since we published our Consultation Paper, a number of statutes have been enacted in England and Wales that criminalise the unauthorised disclosure of personal data. All of these contain a public interest defence for journalists. For example, section 170(3) of the Data Protection Act 2018 provides:

> (3) It is also a defence for a person charged with an offence under subsection (1) to prove that –
>
> > (a) the person acted in the reasonable belief that the person had a legal right to do the obtaining, disclosing, procuring or retaining,
> >
> > (b) the person acted in the reasonable belief that the person would have had the consent of the controller if the controller had known about the obtaining, disclosing, procuring or retaining and the circumstances of it, or
> >
> > (c) the person acted –
> >
> > > (i) for the special purposes,

---

688 Security of Information Act 2001, s 15(5).

689 If the concern relates to a member of the Communications Security Establishment.

690 If the concern does not relate to a member of the Communications Security Establishment.

691 See CP paras 7.123-7.130 and A.113-A.148.

(ii) with a view to the publication by a person of any journalistic, academic, artistic, or literary material, and

(iii) in the reasonable belief that in the particular circumstances the obtaining, disclosing, procuring, or retaining was justified as being in the public interest.

11.68 Section 174(1) defines "special purposes" as including "the purposes of journalism".

11.69 Section 58(2)(i) of the Digital Economy Act 2017 contains a similar formulation. There seems to be a discernible trend in domestic law that when offences which criminalise the unauthorised disclosure of information are enacted they are accompanied by a defence that applies to journalistic activity.

11.70 If a similar model were to be adopted in the official secrets context, careful thought would need to be given to whether "public interest" and "journalist" should be further defined, and if so, how. It is important to note that the ECtHR case law on Article 10 does not depend on a definition of "journalist". Many categories of people – such as academics or bloggers, for example – could be involved in "journalistic activity", broadly defined.

11.71 Section 174 defines one of the "special purposes" as "journalistic activity". There is no further definition of "journalistic activity".

11.72 This defence is characterised by the requirement that the defendant had a reasonable belief that the obtaining, disclosure, procuring or retaining of the information was in the public interest. Whether the belief was reasonable is an objective enquiry and the individual's subjective belief would not be determinative. It appears that this defence does not require an assessment of whether the individual's conduct was in fact in the public interest.

11.73 By way of contrast, the qualification contained in section 58(2)(i) of the Digital Economy Act 2017 applies to a disclosure which consists "of the publication of information for the purposes of journalism, where the publication of the information is in the public interest". This model appears to require an assessment of whether the disclosure was in fact in the public interest, rather than an assessment of whether the individual reasonably believed it to be so.

11.74 In Australian law, section 122.5(6) of the National Security Legislation Amendment (Espionage and Foreign Interference) Act 2018 provides that:

> (6) It is a defence to a prosecution for an offence by a person against this Division that the person communicated, removed, held or otherwise dealt with the relevant information in the person's capacity as a person engaged in the business of reporting news, presenting current affairs or expressing editorial or other content in news media, and:
>
> (a) at that time, the person reasonably believed that engaging in that conduct was in the public interest; or
>
> (b) the person:

(i) was, at that time, a member of the administrative staff of an entity that was engaged in the business of reporting news, presenting current affairs or expressing editorial or other content in news media; and

(ii) acted under the direction of a journalist, editor or lawyer who was also a member of the staff of the entity, and who reasonably believed that engaging in that conduct was in the public interest.

11.75 A person may not reasonably believe that communicating, removing, holding, or otherwise dealing with information was in the public interest if it constitutes one of a number of specified criminal offences.

CONCLUSION

11.76 Our purpose in this section has been to demonstrate that there are various ways such a defence could be drafted. Our preference remains the broad model articulated in this chapter.

11.77 We have noted that a public interest defence provides an important backstop, ensuring compliance with Article 10 in those cases where the mechanisms for investigation and redress are rendered ineffective.

11.78 The defence should be a true public interest defence on the basis that the overriding concern is that an otherwise criminal disclosure can only be justified on the basis that the disclosure was in the public interest. It does not serve the public interest to excuse those who damage national security simply because they believed that the disclosure was in the public interest.

11.79 The legal burden of proving the defence should rest on the defendant. This avoids compounding damaging disclosures of sensitive information, removes a potentially insuperable obstacle from the prosecution, and does not provide an excessively high bar for the defendant. We consider that Article 6 does not preclude such a reverse burden of proof, and domestic case law has confirmed as much.

11.80 The defence will necessarily involve a two-stage analysis: was the subject matter of the disclosure in the public interest, and was the method of disclosure in the public interest. It is perfectly conceivable that a disclosure that was ostensibly in the public interest was disclosed in a more damaging way than was reasonably required. This two-stage test makes explicit what is implicit in attempt to answer the broad question "was the disclosure in the public interest".

Recommendation 33.

11.81 A person should not be guilty of an offence under the Official Secrets Act 1989 if that person proves, on the balance of probabilities, that: (a) it was in the public interest for the information disclosed to be known by the recipient; and (b) the manner of the disclosure was in the public interest. We make no further recommendation beyond this in respect of the form of the defence.

Chapter 12: Recommendations

Recommendation 1.

12.1 We recommend that a new statute – containing modern language and updated provisions – should replace the Official Secrets Acts 1911-1939.

Paragraph 3.9

Recommendation 2.

12.2 In any new statute to replace the Official Secrets Act 1911, the concept of "enemy" in section 1 should be replaced with that of "foreign power". The Canadian definition of "foreign power", including reference to terrorist groups and entities directed by a foreign government, should be used as a starting point for drafting that element of the new provision.

Paragraph 3.32

Recommendation 3.

12.3 In any new statute to replace the Official Secrets Act 1911, the term "safety or interests of the state" should be retained.

Paragraph 3.45

Recommendation 4.

12.4 An individual should only be criminally liable for an espionage offence if he or she has a purpose which he or she knows or has reasonable grounds to believe is prejudicial to the safety or interests of the state.

Paragraph 3.56

Recommendation 5.

12.5 In any new statute to replace the Official Secrets Act 1911, the requirement that the defendant's conduct was capable of benefitting a foreign power should continue to be objectively determined. There should be no requirement to prove that the defendant personally knew or believed that his or her conduct had such capability.

Paragraph 3.70

Recommendation 6.

12.6 The list of prohibited places should be drafted to reflect the modern espionage threat.

12.7 The Secretary of State should have the power, by statutory instrument subject to the affirmative resolution procedure, to amend the list of prohibited places where it is appropriate to do so in the interests of the safety or interests of the state.

12.8 The Secretary of State should be obliged to consider taking steps to inform the public of the effect of any designation order, including, in particular, by displaying notices on or near the site to which the order relates where appropriate.

Paragraph 3.85

Recommendation 7.

12.9 There should continue to be no restriction on who can commit the offences contained in the Official Secrets Act 1911 or in any replacement legislation.

12.10 There should continue to be separate offences of espionage by trespass and espionage by collection or communication of information.

12.11 The espionage by trespass offence should also continue to apply to those who approach, inspect, pass over or enter any prohibited place within the meaning of the Act.

12.12 The collection and communication offence should continue to be capable of being committed not only by someone who communicates information, but also by someone who obtains it.

12.13 References in the Official Secrets Acts 1911 and 1920 to a sketch, plan, model, note and secret official pass word and code word are anachronistic and should be replaced with "document, information or other article". Information should be defined to include any program or data held in electronic form.

Paragraph 3.106

Recommendation 8.

12.14 We recommend that sections 1(2) of the Official Secrets Act 1911 and section 2(2) of the Official Secrets Act 1920 should be repealed.

Paragraph 3.119

Recommendation 9.

12.15 We recommend that section 7 of the Official Secrets Act 1911 and section 2(1) and section 6 of the Official Secrets Act 1920 should be repealed without replacement.

12.16 The offence of doing an act preparatory to espionage should be retained. Save for that, section 7 of the Official Secrets Act 1920 should be repealed.

Paragraph 3.130

Recommendation 10.

12.17 The territorial ambit of the offences contained in the Official Secrets Acts 1911-1939 should be expanded so that they can be committed irrespective of the individual's nationality. The test should be whether there is a "significant link" between the individual's behaviour and the interests of the United Kingdom.

12.18 "Significant link" should be defined to include not only the case where the defendant is a Crown employee or contractor, but also the case where the conduct relates to a site or data owned or controlled by the UK government (irrespective of the identity of the defendant).

12.19 To ensure that sensitive UK assets overseas receive maximum protection, any new definition of "prohibited place" (see recommendation 6) should explicitly provide that such places may be overseas.

Paragraph 3.150

Recommendation 11.

12.20 Those offences under the Official Secrets Act 1989 that relate to Crown servants or government contractors and that require proof or likelihood of damage (section 1(3); section 2(1); section 3(1); section 4(1)) should no longer require such proof or likelihood.

12.21 Instead, there should be an explicit subjective fault element. Further work will be required to determine the most appropriate fault element (ie that the defendant (i) knew; (ii) believed; or (iii) was reckless as to whether the disclosure (a) would cause damage; (b) was likely to cause damage; (c) risked causing damage; or (d) was capable of causing damage).

12.22 Sections 5 and 6 should continue to be based on proof or likelihood of damage.

Paragraph 4.81

Recommendation 12.

12.23 The offence contrary to section 1(1) of the Official Secrets Act 1989 should not be amended to require proof that the disclosure was damaging.

12.24 The "defence", currently contained in section 1(5) of the Official Secrets Act 1989, of not knowing and having no reasonable grounds to believe that the material disclosed related to security or intelligence, should continue to apply.

Paragraph 5.17

Recommendation 13.

12.25 The definition of "member" of the security and intelligence services should be clarified to mean any individual employed or contracted by the security and intelligence services or seconded or attached to them.

12.26 There should be a statutory requirement to publish guidance on the notification process. The guidance should state which categories of office are subject to notification and how an individual can challenge a decision to notify him or her.

Paragraph 5.41

Recommendation 14.

12.27 A maximum sentence of two years' imprisonment does not provide the court with adequate powers in really serious cases.

12.28 Parliament should consider increased maximum sentences for some offences under the Official Secrets Act 1989.

12.29 Consideration should also be given to whether a distinction ought to be drawn in terms of maximum sentence between the offences in sections 1 to 4 of the Official Secrets Act 1989 and the offences in sections 5 to 6.

Paragraph 5.70

Recommendation 15.

12.30 We recommend that the professional bodies responsible for the Codes of Conduct for practising lawyers – the SRA and BSB – consider including explicit guidance on the importance of maintaining confidentiality in cases involving the Official Secrets Acts, and the obligation not to receive disclosures unless they have the appropriate security clearance and premises assurance.

Paragraph 5.127

Recommendation 16.

12.31 Where a person not subject to section 1(1) of the Official Secrets Act 1989 who is not a subject of a relevant criminal investigation makes a disclosure to a qualified lawyer for the purpose of obtaining legal advice, that disclosure should constitute an authorised disclosure, subject to specific safeguards being met.

12.32 The safeguards are as follows: (i) the legal adviser must be subject to professional obligations, either through the Bar Standards Board or the Solicitors Regulation Authority; and (ii) the lawyer to whom the disclosure is made must have undergone security vetting to the appropriate level and systems/premises assurance.

Paragraph 5.136

Recommendation 17.

12.33 We recommend that, where a Crown servant, government contractor or notified person is a suspect in a criminal investigation and makes a disclosure to a qualified legal adviser for the purposes of legal advice, that disclosure should be authorised for the purposes of sections 1-4 of the Official Secrets Act 1989 if the legal adviser has security clearance to the appropriate level, given the nature of the protected information, and has undergone systems/premises assurance.

Paragraph 5.146

Recommendation 18.

12.34 It should be made explicit that prior publication is a factor that ought to be considered by prosecution agencies, courts, and juries when determining whether an unauthorised disclosure was damaging for the purposes of the sections 5 and 6 offences under the OSA 1989.

12.35 It should be made clear that it is not an offence for the purposes of sections 1(3) to 4 to communicate information that has been already communicated to the public or made available to the public with lawful authority.

Paragraph 5.169

Recommendation 19.

12.36 The categories of information currently protected by the Official Secrets Act 1989 should not be narrowed at this time. For any reform of the Official Secrets Act 1989, however, the possibility of defining the categories of information with greater precision ought to be explored as a priority.

Paragraph 5.185

Recommendation 20.

12.37 The categories of information protected by the Official Secrets Act 1989 should not be expanded to include economic information in so far as it relates to national security.

Paragraph 5.205

Recommendation 21.

12.38 The territorial ambit of sections 1 to 4 of the Official Secrets Act 1989 should be amended so that a government contractor or notified person commits an offence when he or she makes an unauthorised disclosure abroad irrespective of whether he or she is a British citizen.

Paragraph 5.222

Recommendation 22.

12.39 There should be a review of unauthorised disclosure offences with the aim, in particular, of creating greater coherence and consistency in terms of the defences available and penalties that apply.

Paragraph 6.27

Recommendation 23.

12.40 If a widescale review of the miscellaneous disclosure offences is conducted, it ought to include section 170 of the Data Protection Act 2018 for the sake of completeness and in an effort to ensure maximum coherence.

Paragraph 6.43

Recommendation 24.

12.41 National security disclosure offences should form part of the review of miscellaneous disclosure offences recommended above.

Paragraph 6.50

Recommendation 25.

12.42 The Protocol on Leak Investigations should be reviewed and updated, in consultation with Government Departments, the Crown Prosecution Service, the Metropolitan Police, the Attorney General, and any other interested parties.

Paragraph 7.39

Recommendation 26.

12.43 Consideration should be given, as part of the review of the Protocol, to an appropriate mechanism for providing oversight of its operation.

Paragraph 7.40

Recommendation 27.

12.44 The Crown Prosecution Service guidance "Prosecuting Cases Where Public Servants Have Disclosed Confidential Information to Journalists" should be updated to reflect developments in case law and to make reference to the Protocol.

Paragraph 7.41

Recommendation 28.

12.45 The Protocol should be published more accessibly online with information stating when it came into force, and detailing any revisions.

Paragraph 7.42

Recommendation 29.

12.46 We recommend that the power conferred on the court by section 8(4) of the Official Secrets Act 1920 ought to be subject to a necessity test, such that the exclusion of members of the public must be necessary for the administration of justice having regard to the risk to national safety (replacing the term used in the 1920 Act: "prejudicial").

Paragraph 7.65

Recommendation 30.

12.47 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 and the judge.

Paragraph 7.79

Recommendation 31.

12.48 We recommend that a separate review be undertaken to evaluate the extent to which the current mechanisms in the criminal trial process strike the correct balance between the right to a fair trial and the need to safeguard sensitive material.

Paragraph 7.100

Recommendation 32.

12.49 An independent, statutory commissioner should be established with the purpose of receiving and investigating allegations of wrongdoing or criminality where otherwise the disclosure of those concerns would constitute an offence under the Official Secrets Act 1989.

12.50 That commissioner would have to constitute an effective investigative mechanism: it would therefore have not only to be independent, but also be able to act expeditiously and have the legal authority to compel cooperation with its investigations.

12.51 There should be a right of appeal by the complainant against decisions of the statutory commissioner. The jurisdiction of the Investigatory Powers Tribunal should be expanded such that it can hear appeals against decisions of the statutory commissioner.

Paragraph 10.108

Recommendation 33.

12.52 A person should not be guilty of an offence under the Official Secrets Act 1989 if that person proves, on the balance of probabilities, that: (a) it was in the public interest for the information disclosed to be known by the recipient; and (b) the manner of the disclosure was in the public interest. We make no further recommendation beyond this in respect of the form of the defence.

Paragraph 11.81

Appendix 1: List of those who responded to the Consultation Paper

1.1 In total, we received 1,251 responses to our Consultation Paper from a broad cross-section of stakeholders. This included many hundreds of responses from individual members of the public, to whom we are grateful. There were too many responses to identify each here, though we should like to note the following professionals, academics and organisations in particular.

GOVERNMENT AND PUBLIC BODIES

1.2 Her Majesty's Government

1.3 Intelligence and Security Committee of Parliament

1.4 Information Commissioner's Office

1.5 DSMA Committee

1.6 Crown Prosecution Service

MEDIA ORGANISATIONS

1.7 News Media Association

1.8 Centre for Journalism

1.9 News UK/News Group Newspapers

1.10 Trinity Mirror (now known as Reach plc)

1.11 Media Lawyers Association

1.12 ITN

1.13 BBC

1.14 Telegraph Media Group

1.15 Associated Newspapers Ltd

1.16 Newsquest Media Group

1.17 Guardian News and Media

1.18 CPU Media Trust

1.19 Society of Editors

1.20 National Union of Journalists

1.21 Channel 4

OTHER LEGAL ORGANISATIONS AND LAW FIRMS

1.22 Bar Council and Criminal Bar Association

1.23 Peters and Peters

1.24 McEvedys Solicitors and Attorneys

OTHER FIRMS

1.25 Newrisk Ltd

NON-GOVERNMENTAL ENTITIES

1.26 Global Witness

1.27 The Institute of Employment Rights

1.28 English PEN/Index on Censorship/Reporters Without Border

1.29 Campaign Against Censorship

1.30 Whistleblowers UK

1.31 Transparency International

1.32 The Courage Foundation

1.33 Open Rights Group

1.34 Campaign for Freedom of Information/Article 19

1.35 Liberty

1.36 UK Open Government Network

1.37 Public Concern at Work

1.38 Compassion in Care

1.39 British Computer Society

ACADEMIC

1.40 Prof Jacob Rowbottom

1.41 Dr Oliver Butler

1.42 Dr Ashley Savage

1.43 Prof David Leigh

1.44 Dr Lesley Phippen

1.45 Dr Dimitris Xenos

1.46 Prof Lorna Woods, Dr Lawrence McNamara and Dr Judith Townend

1.47 Alan Rusbridger (former editor-in chief of the Guardian)

SELECT INDIVIDUAL RESPONSES

1.48 Annie Machon, former MI5 intelligence officer

1.49 Peter Francis, former undercover police officer

CCS0820043516

978-1-5286-2113-7