Law Commission
Reforming the law

Protection of Official Data
Summary

Consultation Paper No 230 (Summary)
February 2017

PROTECTION OF OFFICIAL DATA
EXECUTIVE SUMMARY

BACKGROUND TO THIS CONSULTATION

1.1 The Protection of Official Data project was referred to us by the Cabinet Office in late 2015. We commenced work in February 2016 and will publish our final report in Summer 2017. The public consultation now runs from 2 February 2017 to 3 April 2017 and this summary accompanies the publication of our full consultation paper. The consultation paper and associated documents (including a two page press summary) can be found at http://www.lawcom.gov.uk/project/protection-of-official-data/

1.2 Our comprehensive 300+ page consultation paper contains our analysis of the current domestic and comparative law. We have put paragraph references to our consultation paper in square brackets throughout this document for ease of cross reference. We also reproduce all of our provisional conclusions and consultation questions in full in this summary. They are written in bold text so consultees can easily identify them.

SCOPE OF THIS PROJECT

1.3 Most people are aware that the law criminalises the unauthorised disclosure of specified categories of official information. Most of those criminal offences apply only to those people working within or alongside Government who have been trained in how to handle sensitive information. A quite separate set of criminal offences deal with any person who engages in activity that is usually known as espionage: where an individual seeks to gain access to sensitive information with the intent to prejudice the safety or interests of the state usually for the benefit of a foreign power.

1.4 We were asked, as an independent, non-governmental body of law reform experts with extensive experience of conducting public consultations, to examine the effectiveness of the law in this area and assess whether there are any deficiencies that undermine the protection of official information.

1.5 In producing our provisional conclusions we conducted an extensive review of the law, commissioned a comparative study of the law in five jurisdictions and engaged in preliminary fact finding with various government departments and non-governmental organisations.[1]

1.6 This project has provided a unique opportunity independently to review a difficult area of law, some of which has not been subjected to rigorous independent scrutiny for over a century.

[1] Appendix B contains a list of the departments, organisations and individuals that we have sought views from during our preliminary fact finding.

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

1.8 Finally by way of introduction, we acknowledge at the outset that some people disagree with the proposition that the unauthorised disclosure of information should be criminalised. Our terms of reference did not permit us to question this underlying assumption. We do believe, however, that certain categories of information require the effective protection of the criminal law and that it is necessary to ensure sensitive information is safeguarded against those whose goal is to prejudice the safety and security of the United Kingdom.

LEGAL BACKGROUND TO THE PROTECTION OF OFFICIAL DATA

1.9 The most well-known legal provisions in this area are the Official Secrets Acts 1911, 1920, 1939 and 1989. This review considers the protection offered by those Acts but also examines other criminal offences that protect against unauthorised disclosures of information held by government. We also 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. Given that almost all of the relevant legislation was enacted long before the Human Rights Act 1998 came into force, we have also sought to assess the extent to which the relevant provisions comply with the European Convention on Human Rights.

CHAPTER 2 - OFFICIAL SECRETS ACTS 1911, 1920 AND 1939

2.3 Chapter 2 of the Consultation Paper analyses the provisions contained in the Official Secrets Acts 1911, 1920, and 1939. This legislation is concerned with espionage, which could be roughly described as the gathering of non-public information, usually through covert means, usually for the benefit of a foreign power. If this information is obtained by those with no right to access it, damage to the national interest can be caused.

2.4 Problems with the current law identified and discussed in the consultation paper include the following key elements of the espionage offences:

<u>The need for an enemy</u>

2.5 The offences in sections 1(1)(b) and 1(1)(c) of the Official Secrets Act 1911 require proof that the information supplied or obtained was calculated to be, or might be, or is intended to be directly or indirectly useful to “an enemy”. Our initial fact finding with stakeholders suggests that this term causes problems in practice. This finding reflects a point made a number of years ago by the Intelligence and Security Committee of Parliament.[2]

[2] Intelligence and Security Committee of Parliament: Annual Report 2003-2004 (2004) Cm 6240, p 43.

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

2.7 **We provisionally conclude that the inclusion of the term "enemy" has the potential to inhibit the ability to prosecute those who commit espionage and ask consultees whether they agree [2.113]**

2.8 We consider that the problem can be met by referring to a foreign power rather than an enemy and defining foreign power to reflect the modern geopolitical world. The increasing power of companies within state structures, and complex governance models can make it difficult to determine whether an entity such as a company is acting in a private capacity or as an emanation of the state. Further, in some instances it is clear that companies may be under state control, or have a majority stake owned by governments, where the nature of the investments is non-commercial, but rather an instrument of policy making. It is desirable that any new offence should be flexible in accommodating the different ways in which foreign power may be exercised. A failure to do so would render the offence ineffective. We draw upon a list of entities that might be treated as a foreign power in the US Espionage Statutes Modernization Bill and ask consultees:

2.9 **Is the list of foreign entities contained in that Bill a helpful starting point in the UK context? Do consultees have views on how it could be amended? [2.144]**

2.10 Following our emphasis throughout the Consultation Paper we consider that criminal liability should require subjective proof that the defendant must know or believe that his conduct (engaging in gathering information etc) might benefit a foreign power.

2.11 We provisionally conclude that an offence should only be committed if the defendant knew or had reasonable grounds to believe his or her conduct was capable of benefiting a foreign power.

2.12 Aside from replacing the requirement of enemy with one of foreign power, we believe that several other elements of the offence must be reformed and redrafted in more modern form.

2.13 We conclude that any redrafted offence ought to have the following features:

(1) Like the overwhelming majority of criminal offences, there should continue to be no restriction on who can commit the offence [in other words it should not be restricted to civil servants or British citizens] This is true of the current law and therefore does not represent a change;

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

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

Do consultees agree? [2.123]

2.14 To reformulate the offence, we also need to examine:

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

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

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

<u>The term "safety or interests of the state"</u>

2.15 At present it must be proved that the conduct (engaging in gathering information etc) is performed for the purpose of prejudging the "safety or interests of the state". It could be argued that this gives the offence too broad a scope if the 1911 Act requirement for the information to be "useful to an enemy" is replaced by a broader concept extending to any "foreign power". One way of providing a greater degree of specificity is to use the term "national security" rather than "safety or interests".

2.16 **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"? [2.129]**

2.17 At present what is arguably the most important element of the offence – prejudice to the safety or interests of the state – has no subjective fault element at all. Given the seriousness of the offence, we believe it is important for this element of the offence to incorporate a subjective fault element.

2.18 **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? [2.137]**

2.19 To recap the proposals in this section, a person would commit an offence if he or she:

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

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

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

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

2.20 It is important to point out that any reformulated offence would be capable of being committed in inchoate form: attempts, conspiracy and assisting and encouraging espionage would all remain criminal. Again, this is true of the current law and is not a change.

The focus on military installations

2.21 Section 1(1)(a) of the Official Secrets Act 1911 makes it an offence for a person, for any purpose prejudicial to the safety or interests of the state to approach, inspect, pass over, be in the neighbourhood of, or enter any prohibited place as that term is defined in the Act.

2.22 Section 3 of the Official Secrets Act 1911 contains an extensive list of "prohibited places".[3] Our initial fact finding with stakeholders, however, suggests that this list is under inclusive. This is because:

(1) The primary focus of the list is upon sites that are military in nature. In the modern era sensitive information that needs protection from being targeted is not only held on sites which are military in nature, but upon sites which may have a variety of uses.

(2) The legislation does not protect sites that store sensitive economic information that may also be targeted by those with intent to injure the national interest.

(3) There is no reference to the critical national infrastructure.

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

2.24 The under-inclusive list of prohibited places in the Official Secrets Act 1911 stands in contrast to the list of protected sites in the Serious Organised Crime and Police Act 2005. One way to remedy this problem is to rely upon the approach taken in the Serious Organised Crime and Police Act 2005, whereby only those sites that relate to national security can be designated. This would ensure the legislation is capable of meeting contemporary challenges. Such a list would be enacted in primary legislation, but would be capable of amendment by way of the affirmative resolution procedure.

[3] Although the list may be amended, this power has been exercised infrequently over the years.

2.25 **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 was in the interests of national security to do so. Do consultees agree? [2.163]**

Archaic provisions

2.26 As was typical of the Edwardian era, the legislation is drafted in archaic fashion and contains a number of provisions that may have been necessary in 1911, but seem somewhat quaint today; for example, possessing a counterfeited die, seal or stamp resembling one used by a Government Department. We are unaware of this offence ever being prosecuted. Whilst we accept that these things are in need of protection, we believe it would be preferable to use a sufficiently generic term. This would minimise the possibility that there are gaps in the legislative protection. We provisionally conclude that:

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

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

2.29 **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? [2.186]**

The territorial ambit of the offences

2.30 The Official Secrets Act 1911 provides that an offence can be committed by someone acting outside the United Kingdom if he or she is a British Officer or subject, which means that it has extraterritorial effect. Although the legislation applies outside the United Kingdom, it only does so if the person who engaged in the prohibited conduct is a British Officer or subject. We have provisionally concluded that the territorial ambit of the Official Secrets Act 1911 is insufficient to offer adequate protection to sensitive assets abroad. For this reason the territorial ambit of the offences ought to be expanded so that the offences can be committed irrespective of whether the person 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.

2.31 **We conclude that 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? [2.175]**

The means of proving espionage offences.

2.32 One of the aims of the Official Secrets Acts 1911 and 1920 was to ease the prosecution's burden in respect of proving certain elements of the offences in the Official Secrets Act 1911.

2.33 For example, the effect of section 1(2) of the Official Secrets Act 1911 is that the prosecution does need to prove beyond reasonable doubt that the defendant had a purpose prejudicial to the interests of the state. It suffices that it *appears* that the defendant had such a purpose from his "known character as proved". One reason why this might be objectionable is that it may introduce a standard of proof less than beyond reasonable doubt. Furthermore, it is generally accepted that deeming provisions such as these have no place in the criminal law.

2.34 To take another example, section 2(2) of the 1920 Act, in some cases, explicitly places a burden upon the defendant to prove on the balance of probabilities that he or she has not been in communication with a foreign agent. If the defendant fails to discharge this burden, then he or she will be presumed to have been in communication with a foreign agent, which in turn provides evidence of commission of one of the offences contained in section 1 of the Official Secrets Act 1911.

2.35 We do not underestimate the difficulty in proving the commission of espionage offences, but provisions such as those contained in the Official Secrets Acts 1911 and 1920 are difficult to reconcile with the principle that the prosecution bear the burden of proof. In this regard, it is important to bear in mind that the means of investigating espionage are much more advanced than they were when the Official Secrets Acts 1911 – 1939 were enacted. We seek consultees views:

2.36 **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? [2.190]**

Conclusion

2.37 In terms of how our amendments could be enacted in law, we provisionally conclude that the reforms we have discussed could form the basis of a new Act. This would entail repealing the Official Secrets Acts 1911-1939 and replacing them with a new, modern statute. Rather than simply making amendments to the 1911 Act, this would have the advantage that the title of the legislation would convey the purpose of the Act. It would also provide the opportunity to ensure that the legislation is fit for purpose in the digital era and ensure that it is drafted so as to be compliant with the European Convention on Human Rights.

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

CHAPTER 3 - THE OFFICIAL SECRETS ACT 1989

3.2 Chapter 3 of the consultation paper analyses the provisions contained within the Official Secrets Act 1989 and their development..

3.3 The Official Secrets Act 1989 criminalises the unauthorised disclosure only of specified categories of information, namely security and intelligence, defence, international relations, crime and special investigation powers and information entrusted in confidence to or by other states or international organisations. Unusually, the Official Secrets Act 1989 only applies, for the most part, to those who are members of the security and intelligence agencies, Crown servants, government contractors and those who have been notified by the Secretary of State that they are subject to the Act.[4]

3.4 Our research suggests that the Official Secrets Act 1989 suffers from a number of problems. Some of these problems are attributable to the disparate nature of disclosure offences and the lack of rationality and coherence between them. Other problems are attributable to the manner in which the Official Secrets Act 1989 was drafted and the fact it was drafted before the digital era. Our paper asks for consultees' views on a number of ways the current law could be amended so as to rectify these problems.

The need to prove damage

3.5 All the offences in the Official Secrets Act 1989, apart from the offences in sections 1(1) and 4(3) require the prosecution to prove that the unauthorised disclosure was damaging or was likely to cause damage.

3.6 This is a problem, however, as it may have the effect of increasing the damage caused by the initial disclosure of information. As Lord Nicholls said in in *Shayler*:

> Damage already done may well be irreparable, and the gathering together and disclosure of evidence to prove the nature and extent of the damage may compound its effects to the further detriment of national security.[5]

3.7 These provisions stand in contrast to the offences identified in Chapter 4 which do not require proof that the disclosure was damaging. This includes offences that criminalise the disclosure of information relating to national security and which carry a higher maximum sentence than the offences contained in the Official Secrets Act 1989. The Official Secrets Act 1989 is therefore not representative of how such disclosure offences are typically drafted. For example, section 79 of the Anti-terrorism, Crime and Security Act 2001 criminalises the unauthorised disclosure of information the disclosure of which might prejudice the security of any nuclear site with the intention of prejudicing that security or being reckless as to whether the disclosure might prejudice that security. There is no requirement to prove that the security of any nuclear site was in fact prejudiced. The offence carries a maximum sentence of 7 years' imprisonment if tried in the Crown Court.

[4] By virtue of section 1(6) of the Official Secrets Act 1989 notification that a person is subject to section 1(1) of the Act will be served by a Minister of the Crown 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 or she should be subject to the provisions of that subsection.

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

3.8 **We provisionally conclude that, as a matter of principle, it is undesirable for those who have disclosed information contrary to the Official Secrets Act 1989 to be able to avoid criminal liability due to the fact that proving the damage caused by the disclosure would risk causing further damage. Do consultees agree? [3.148]**

The structure and nature of the offences

3.9 The way the offences are drafted no longer reflects how they are applied in practice. On their face, the offences contained in the Official Secrets Act 1989 appear to be offences of strict liability, as there is no need to prove, for example, that the defendant *intended* to cause damage to the capability of the armed forces of the Crown in order for him or her to be guilty of an offence contrary to section 2. It is not accurate, however, to describe the offences as being offences of strict liability. This is because each of the offences in sections 1 – 3 of the Official Secrets Act 1989 contains a defence for the defendant to prove that at the time of the alleged offence, he or she did not know and had no reasonable cause to believe that the information, document or article in question related to a protected category of information and/or that its disclosure would be damaging.

3.10 In *Keogh* the Court of Appeal held that, in order to ensure the offences comply with the right to a fair trial which is enshrined in Article 6 of the European Convention on Human Rights, it is necessary for the prosecution to prove that the defendant knew or had reasonable cause to believe that the information that was disclosed fell within a protected category and that its disclosure would cause damage or would be likely to cause damage.[6] The court did state, however, that someone could commit an offence without inviting the jury to engage in a subjective assessment of the defendant's state of mind. The court therefore adopted a wholly objective interpretation of this fault element.

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

3.12 For example, it could be argued that the individual who discloses information knowing that that disclosure is capable of damaging security and intelligence, defence or international relations should be subject to a higher maximum sentence than the individual who has reasonable grounds to believe that that disclosure is capable of damaging security and intelligence, defence or international relations.

3.13 **We provisionally conclude that proof of the defendant's culpable state of mind should be an explicit element of the offence contained in the Official Secrets Act 1989. Do consultees agree? [3.151]**

How the offences might be restructured

3.14 As we have already discussed, most of the criminal offences currently contained in the Official Secrets Act 1989 require proof that the defendant's unauthorised disclosure caused or was likely to cause, a prohibited result: damage to the relevant interest (defence, international relations etc).

[6] *Keogh* [2007] EWCA Crim 528; [2007] 1 WLR 1500.

3.15 One option that we believe would remedy the difficulty of being unable to prove that the disclosure caused or was likely to cause the requisite damage is to refocus the offences so that they depend on the defendant's conduct and culpable state of mind when engaging in that conduct. Such offences are often described as being drafted in the "inchoate mode". For example the offence of burglary is committed if a person enters a building as a trespasser with the intention of committing either theft, grievous bodily harm, or criminal damage, irrespective of result. There is no need to prove that a theft etc. took place: it is the willingness to engage in the conduct with intent to steal that justifies criminalising that act as burglary. Another example is the Fraud Act 2006 which criminalises fraudulent conduct, irrespective of whether it succeeds in deceiving anyone and irrespective of whether it led to the defendant obtaining any property.[7]

3.16 There are clear and long established precedents for moving from a result orientated offence to a model based on the culpable state of mind. We are keen to ensure, however, that the threshold of culpability that must be crossed before an individual commits a criminal offence for disclosing information without lawful authority is not lowered. One way we believe this aim could be achieved is to redraft the offences so that they explicitly incorporate a *subjective* fault element. Such a change would mean that an individual could only be liable for the unauthorised disclosure offences if he or she knew or believed that the disclosure in question was capable of damaging a specified interest (such as defence or international relations). This would be a subjective question, in contrast to the current law, which requires an objective evaluation.

3.17 As an example of how we believe the offences could be redrafted we offer the following:

> A person commits an offence if he or she intentionally makes an unauthorised disclosure of information relating to security and intelligence, knowing or having reasonable grounds to believe that that disclosure is capable of damaging security and intelligence.
>
> A person commits an offence if he or she intentionally makes an unauthorised disclosure of information relating to defence, knowing or having reasonable grounds to believe that that disclosure is capable of damaging defence.
>
> A person commits an offence if he or she intentionally makes an unauthorised disclosure of information relating to foreign relations, knowing or having reasonable grounds to believe that that disclosure is capable of damaging international relations.

3.18 **We welcome consultees' views on the suitability of shifting to non-result based offences to replace those offences in the Official Secrets Act 1989 that require proof or likelihood of damage. [3.164]**

[7] For example, the offence of fraud by false representation under section 2(1) of the Fraud Act 2006 is committed when a person dishonestly makes a false representation and intends either to make a gain or cause loss to another, regardless of whether the gain or loss did in fact occur.

3.19 Elements of the offences differ when it comes to members of the security and intelligence services and notified persons. We have provisionally concluded that the historical reasons for treating membership of the security and intelligence services differently still apply: specifically that membership carries with it a special and inescapable duty of secrecy and such disclosures may reduce public confidence in the services' ability to carry out their duties effectively and loyally. This means that a member of the security and intelligence agencies or a notified person would be liable without the need to prove that he or she knew or had reasonable cause to believe the disclosure was capable of being damaging.

3.20 **We provisionally conclude that when it comes to members of the security and intelligence agencies and notified persons, the offences should continue to be offences of strict liability. [3.167]**

Delineating who is subject to the provisions in the Official Secrets Act 1989

3.21 The offences in sections 1-4 of the Official Secrets Act 1989 only apply to:

(1) Members and former of the security and intelligence services.

(2) Persons notified they are subject to the provisions of the Act.

(3) Crown servants and former Crown servants.

(4) Government contractors.

3.22 Stakeholders have suggested that there are a number of problems with the way in which the legislation brings certain officeholders within its remit. First, the meaning of the term "member of the security and intelligence services" is obscure. For example it is unclear whether the term "member" is intended to be synonymous with employee or whether it is intended to be broader. There are similar problems defining "Crown servant".

3.23 Secondly, the concept of being a "notified person" and the process by which the Minister serves notification in writing to designate such a person is slow and does not reflect the fact that sometimes a person must be notified at short notice. Secondly, it assumes the list of those who ought to be notified remains largely static. In practice, however, this is not the case, given the internal restructuring that can take place within a department.

3.24 The experience of using the notification process since the Official Secrets Act 1989 was enacted suggests that it does not work as well as it should.

3.25 **The process for making individuals subject to the Official Secrets Act 1989 is in need of reform to improve efficiency. Do consultees agree? Do consultees agree? [3.178]**

3.26 **If consultees agree with our previous provisional conclusion, do consultees have a view on whether these options would improve the efficiency of the process for making individuals subject to the Official Secrets Act 1989?**

(1) Member of the security and intelligence services – As we have discussed, it is not entirely clear what is intended to be meant by the term "member". One option is to amend the term to clarify that

employees, seconded and attached staff, in addition to those working under a contract of service, fall within the scope of the offence in section 1(1).

(2) Notified person – We have provisionally concluded that notification does serve a useful function and ought to be retained. We do believe, however, that there are two ways the process could be improved. First, new guidance could be issued clarifying when an individual ought to be subject to notification. Secondly, the length of time a notification is in force could be lengthened. It is possible, however, to envisage more fundamental reform that would further reduce the administrative burden. One option is to specify the types of post that ought to be subject to notification. Rather than focusing upon the individual, the focus would be on the post. A second option would be to replace the notification provisions and expand the scope of section 1(1) to anyone who has, or has had access to security and intelligence information by virtue of their office or employment or contract of services.

(3) Definition of Crown servant – We provisionally conclude that the process for expanding the definition of Crown servant ought to be streamlined and that it should be possible to make an officeholder a Crown servant for the purposes of the Official Secrets Act 1989 by way of primary legislation, in addition to the process set out in section 12 of the Act. [3.179]

Maximum sentence

3.27 The maximum sentences available for offences in the Official Secrets Act 1989 appear low when compared to other offences that criminalise the unauthorised disclosure of information. For example, it is an offence punishable by up to two years' imprisonment for an employee of the National Lottery Commission to disclose certain information that has been supplied by Her Majesty's Commissioners for Revenue and Customs that relates to a person whose identity is specified in the information or whose identity can be deduced from the information. This is the same maximum sentence available for an unauthorised disclosure that, to take one example, damages the capability of the armed forces to carry out their tasks.

3.28 By way of contrast with a more modern offence of a similar focus, it is an offence punishable by up to five years' imprisonment for a Crown servant to disclose without authorisation anything to do with the existence or implementation of certain warrants granted pursuant to the Investigatory Powers Act 2016, including the content of intercepted material and related communications data.

3.29 When compared with these other disclosure offences, it could be argued that the maximum sentence available for the offences in the Official Secrets Act 1989 may not adequately reflect the culpability in the most egregious cases caused by an unauthorised disclosure of information that causes damage to the interests listed in the 1989 Act. The maximum sentence of 2 years' imprisonment is also low compared with similar offences in other jurisdictions. For example, the maximum sentence for making an unauthorised disclosure in Canadian law under the Security of Information Act 2001 is 14 years' imprisonment. We are not, however, suggesting that this is a suitable maximum penalty.

3.30 In the digital age, the volume of information that can be disclosed without authorisation is much greater than when the Official Secrets Act 1989 was originally drafted. It could be argued that this means that the ability to cause damage to the national interest and the risk of such damage occurring has also increased.

3.31 **We provisionally conclude that the maximum sentences currently available for the offences contained in the Official Secrets Act 1989 are not capable of reflecting the harm and culpability that may arise in a serious case. Do consultees agree? [3.189]**

Receiving legal advice

3.32 A potential problem arises where a person is suspected of an offence and wants to seek legal advice. It has been argued that the Official Secrets Act 1989 has the potential to interfere with a defendant's unfettered right to instruct his or her legal advisors.[8] A suspect or person charged with an offence contrary to the Official Secrets Act 1989 might potentially commit further offences when instructing their legal advisors. In instructing their legal advisors, the defendant, a former member of the security and intelligence services for example, might disclose information that relates to security or intelligence. Unless the defendant sought authorisation before making those disclosures, they would commit an offence under section 1(1) of the Official Secrets Act 1989. the problem arises because the offence is one of "disclosure" which is not defined to mean "to make public", but includes "parting with possession of".

3.33 We believe that there are ways this issue could be rectified. The issue of potentially committing further criminal offences when instructing legal advisors has arisen recently in the context of the Investigatory Powers Act 2016. There are sections in the Investigatory Powers Act 2016 that, when commenced, will impose a duty not to make unauthorised disclosures. Failure to comply with this duty is a criminal offence. Certain disclosures, however, are categorised as exempt disclosures. One category of exempt disclosure relates to a disclosure that is made to a professional legal adviser by their client for the purpose of receiving legal advice.

[8] A Bailin, "The last Cold War statute" (2008) *Criminal Law Review* 625, p 629.

3.34 We believe that a similar approach could be taken in the present context. To avoid a gap in the protection the legislation is intended to afford sensitive information, we would expect a disclosure only to constitute an "exempt disclosure" if it was made to a qualified solicitor, barrister or legal executive with a current practising certificate, it was made for the purpose of receiving legal advice in relation to proceedings for an offence contrary to the Official Secrets Act 1989, it was not made with the intention of furthering a criminal purpose and it complied with any vetting and security requirements as might be specified

3.35 **A disclosure made to a professional legal advisor who is a barrister, solicitor or legal executive with a current practising certificate for the purposes of receiving legal advice in respect of an offence contrary to the Official Secrets Act 1989 should be an exempt disclosure subject to compliance with any vetting and security requirements as might be specified. Do consultees agree? [3.197]**

Prior publication

3.36 It has been suggested that it is problematic for the Official Secrets Act 1989 to contain no express defence of prior publication.[9]

3.37 One option to deal with this possibility is for a defence to be available if the defendant proves that the information was already *lawfully* in the public domain as a matter of fact, for example because it was disclosed as a result of a request made under the Freedom of Information Act 2000 and no exemption was invoked to justify not disclosing the information. In this context, we believe that “in the public domain” should mean that the information in question had become widely disseminated to the public.

3.38 **We provisionally conclude that a defence of prior publication should be available only if the defendant proves that the information in question was in fact already lawfully in the public domain and widely disseminated to the public. Do consultees agree? [3.204]**

The categories of information protected by the legislation

3.39 It has been argued that the categories of information protected by the Official Secrets Act 1989 raise difficult issues of interpretation[10] and are too wide.[11] For example, the category protected by section 3 of the Official Secrets Act 1989, international relations, has been singled out as being “troublingly wide”.[12]

3.40 We have received no evidence, however, to substantiate the view that the categories of information encompassed by the Official Secrets Act 1989 are too broad. Bearing in mind the necessity of ensuring that sensitive information does not lose the protection of the criminal law, we would nevertheless welcome consultees’ views on whether the categories should be narrowed and, if so, how.

[9] A Bailin, “The last Cold War statute” (2008) *Criminal Law Review* 625, p 629.

[10] A Bailin, “The last Cold War statute” (2008) *Criminal Law Review* 625, p 629.

[11] G Robertson, *Freedom, the Individual and the Law* (1993), pp 168-173.

[12] For discussion, see G Robertson, *Freedom, the Individual and the Law* (1993), p 170.

3.41 **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. [3.209]**

3.42 One specific issue that has been brought to our attention and that we believe merits further consideration, is the fact sensitive economic information is currently not protected by the Official Secrets Act 1989.

3.43 Whilst being mindful of the need to ensure that the legislation only encompasses information the disclosure of which could damage the national interest, we invite consultees' views on whether information that relates to the economy ought to be brought within the scope of the legislation, bearing in mind the need to ensure that the categories are not defined too broadly.

3.44 One way to define this category is to specify that it only encompasses information that affects the economic well-being of the United Kingdom in so far as it relates to national security. This formulation is utilised in the Investigatory Powers Act 2016, which was recently approved by Parliament. This term is used in the context of the grounds upon which the Secretary of State may issue a targeted interception warrant or a targeted examination warrant. Given the context in which this term is used, it is not surprising that it is narrowly defined. Consultees may take the view, however, that a broader definition is desirable to maximise legislative protection. It is for that reason that we are seeking consultees' views on the suitability of this term in the context of criminal offences intended to safeguard official information.

3.45 **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? [3.214]**

<u>The territorial ambit of the offences</u>

3.46 The Official Secrets Act 1989 represents an exception to the rule that the criminal law is territorial. This is because an individual who is a British citizen or Crown servant can commit an offence contrary to the Official Secrets Act 1989 even if he or she is outside the United Kingdom when the information in question was disclosed without authorisation.[13] A person who is not, however, a British citizen or Crown servant does not commit an offence if he or she discloses the information outside the United Kingdom. This is true even if he or she is a "notified person", as defined in section 1 of the Official Secrets Act 1989. We believe it is necessary to consider the extent to which this creates a gap in the protection the legislation affords sensitive information, particularly now that digital advances give people the ability to store and transfer large quantities of information with relative ease.

3.47 A possible approach is provided by section 11(2) of the European Communities Act 1972 which creates an offence that applies to members of the European Atomic Energy Community institutions or committees irrespective of their nationality, or the geographical location where classified information is disseminated.[14] Under these provisions the information does not lose its protection simply because the defendant was abroad when he or she made the unauthorised disclosure.

[13] M Hirst, *Jurisdiction and the Ambit of the Criminal Law* (2003), p 223-224.

[14] M Hirst, *Jurisdiction and the Ambit of the Criminal Law* (2003), p 224.

3.48 **The territorial ambit of the offences contained in the Official Secrets Act 1989 should be reformed to enhance the protection afforded to sensitive information so that the offence would apply irrespective of whether the unauthorised disclosure takes place within the United Kingdom and irrespective of whether the Crown servant, government contractor or notified person who disclosed the information was a British citizen. Do consultees agree? [3.225]**

Conclusion

3.49 The above discussion highlights why we believe a fundamental overhaul of the Official Secrets Act 1989 would be the optimal solution to the deficiencies that we have identified. They include; the fact that the title does not convey the distinct purpose of the legislation, the misleading use of the word "secret" and the risk that further amending the existing law creates greater incoherence. This latter consideration is especially important given that incoherence could undermine the purpose of the legislation.

3.50 Our views echo the recommendations of the Franks Committee and the 2004 conclusions of the Security and Intelligence Committee of Parliament that "the time has come to consider whether a new Act would be the proper way forward".[15]

3.51 **The Official Secrets Act 1989 ought to be repealed and replaced with new legislation. Do consultees agree? [3.231]**

CHAPTER 4 - MISCELLANEOUS UNAUTHORISED DISCLOSURE OFFENCES

4.1 Our consultation paper identifies over one hundred offences which deal with unauthorised disclosure and are contained in legislation other than the Official Secrets Acts 1911-1939; or 1989, referred to for convenience as "miscellaneous unauthorised disclosure offences". Section 55 of the Data Protection Act 1998 is the most well-known and the most often invoked offence of this type.

4.2 Broadly speaking, these miscellaneous offences fall into two categories. The first category contains those offences which criminalise the disclosure of personal information held by public bodies, broadly defined. The second category contains those offences that criminalise the unauthorised disclosure of information concerning national security, such as information that relates to the enrichment of uranium.

4.3 We consider some of the difficulties with the law relating to the disclosure of personal information and ask whether consultees agree with our assessment that a full review of personal information disclosure offences is needed. The difficulties we have identified with the current law are examined comprehensively and include, for example, lack of uniformity in the drafting of the current law; inconsistency around whether consent is needed to commence prosecution and lack of uniformity around whether the recipient of the information is criminalised.

[15] *Security and Intelligence Committee, 2003-2004 Annual Report,* Cm 6240, p 43. The Committee as currently constituted has expressed no view on the Official Secrets Acts 1911-1989.

4.4 **Do consultees have a view on whether a full review of personal information disclosure offences is needed? [4.59]**

4.5 This chapter also examines some issues that our research has uncovered and which relate to the offence contained in section 55 of the Data Protection Act 1998.

Section 55 of the Data Protection Act 1998

4.6 Section 55 makes it an offence knowingly or recklessly to obtain, or to procure the disclosure to another of personal data without the consent of the data controller. This is a freestanding offence in the sense that, unlike most of the offences examined in the above section, it does not accompany a statutory information gateway. The offence can be committed by individuals in both the public and private sectors and the maximum sentence on conviction, either summarily or on indictment, is an unlimited fine. Prosecutions under section 55 of the Data Protection Act 1998 can only be brought by the Information Commissioner, or by the Crown Prosecution Service with the consent of the Director of Public Prosecutions.

4.7 Two important reforms to section 55 of the Data Protection Act 1998 Act were included in the Criminal Justice and Immigration Act 2008. First, section 77 of the 2008 Act gives the Secretary of State the power to make section 55 of the 1998 an imprisonable offence with a maximum sentence of 12 months' imprisonment and/or a fine on conviction in the magistrates' court; and two years' imprisonment and/or a fine on conviction in the Crown Court. Before exercising the power to bring this provision into force, the Secretary of State must consult with the Information Commissioner, appropriate media organisations and other appropriate persons.[16] Although section 77 of the 2008 Act has been granted the Royal Assent, the Secretary of State has not yet exercised the power to bring it into force.

4.9 Secondly, section 78 of the 2008 Act inserts a new statutory defence into section 55 of the Data Protection Act 1998. This defence may be pleaded if the individual who disclosed the personal data was acting with a view to publishing "journalistic, literary or artistic material"; and with the reasonable belief that the disclosure, obtaining or procuring was in the public interest. Section 78 is not yet in force.

4.10 Our consultation paper identifies some problems relating only to the Data Protection Act 1998. These problems including the maximum available sentence (currently a fine) which does not necessarily seem capable of reflecting adequately the seriousness of the offence and the fact that the data controller is the victim of the unauthorised disclosure, rather than the individual whose personal data has been disclosed.

4.11 Given the problems we have identified with the offence, our provisional conclusion is that section 55 requires review to assess the extent to which it adequately protects personal information.[17]

[16] Criminal Justice and Immigration Act 2008, s 77(4)

[17] Although the offence in section 55 contains a number of deficiencies, we believe it is also worthy of note that it does demonstrate that it is possible to craft an overarching offence that protects personal information.

4.12 **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? [4.85]**

National security disclosure offences

4.13 The label "national security disclosure offence" encompasses those offences that criminalise the unauthorised disclosure of information that has implications for national security, generally speaking. The limited number of offences we have found criminalise disclosures of information concerning nuclear energy and uranium;[18] and information useful to an enemy.[19] We acknowledge that this is not an exhaustive list.

4.14 Given that there are fewer of them and they encompass distinct categories of information, the inconsistencies between these offences are not as extensive as those we examined in the previous section. There are, however, some inconsistencies in sentence and in approach, for example there is no consistency of approach as to whether consideration of damage is necessary in national security disclosure offences. We have been unable to discern any principled reason to explain this inconsistency of approach.

4.15 **Do consultees have a view on whether national security disclosure offences should form part of a future full review of miscellaneous unauthorised disclosure offences? [4.111]**

CHAPTER 5 - PROCEDURAL MATTERS RELATING TO INVESTIGATION AND TRIAL

5.2 Chapter 5 of our consultation paper examines a number of procedural matters that relate specifically to prosecutions for offences contrary to the Official Secrets Acts that we believe are worthy of detailed consideration. In particular we examine:

(1) The so-called "Gateway process", which is the standard procedure adopted before any investigation for an offence contrary to the Official Secrets Acts is initiated.

(2) In relation to the trial, need to ensure the continued confidentiality of any sensitive information that may have to be placed before the jury.

(3) Finally, the broader question of whether more extensive reform is needed of the criminal procedure that is adopted in trials that require sensitive information to be placed before a jury.

[18] Anti-terrorism, Crime and Security Act 2001, s 79; Uranium Enrichment Technology (Prohibition on Disclosure) Regulations 2004/1818 brought into force by virtue of Anti-terrorism, Crime and Security Act 2001, s 80; and Nuclear Industries Security Regulations 2003/403, regs 22 and 25.

[19] Armed Forces Act 2006, ss 1 and 17.

The Protocol

5.3 The process for conducting investigations into potential offences under the Official Secrets Acts was changed significantly as a result of a report published by Her Majesty's Chief Inspector of Constabulary in 2009.[20] This report followed a review of the Metropolitan Police involvement in a high profile investigation into a series of unauthorised disclosures emanating from the Home Office.

5.4 The overarching conclusion of Her Majesty's Inspectorate of Constabulary was that the police should only be involved in the investigation of unauthorised disclosures of information when there are reasonable grounds to believe that either an offence under the Official Secrets Act 1989 or some other serious criminal offence has been committed.[21] Appended to the report was a seven stage protocol designed to assist inform police and other stakeholders of the criteria for involving the police in future investigations, irrespective of who had committed the alleged criminal offence.

5.5 The seven step process, as recommended by Her Majesty's Inspectorate of Constabulary and subsequently adopted by the Government, is reproduced in full in our consultation paper at paragraphs 5.14 to 5.15. The Protocol makes it clear that the independence of the police from the Executive (the Cabinet Office and the Government more generally) must be maintained. In determining whether a particular allegation meets the threshold to move through "the Gateway" onto police investigation, a panel of SPOCs (Single Points of Contact) from a range of organisations including the Cabinet Office and the Metropolitan Police Service will assess the strength of the intelligence/evidence package.

5.6 The Protocol is intended to reflect the fact that, generally speaking, the unauthorised disclosure of information is not a criminal offence. Therefore the police should only be invited to conduct an investigation if the high threshold of criminality is met.

5.7 One potential problem we have identified with the gateway process is that it fulfils a number of different functions. To take a few of the different examples we discuss in our consultation paper; it is designed to maintain consistency of handling approach across government, to filter out less serious allegations, to ensure a proportionate response and also to retrieve information that could jeopardise national security as quickly as possible.

5.8 We believe there is the potential for these different functions to conflict. For example, in seeking to ensure that sensitive information is retrieved and secured as quickly as possible so as to minimise the risk to national security, there is the risk that evidence may be contaminated. This may undermine the ability to prosecute the individual who disclosed the information.

Provisional conclusion 18

[20] Her Majesty's Inspectorate of Constabulary, *Review of the Lessons Learned from the Metropolitan Police Service's Investigation of Home Office Leaks* (2009).

[21] Her Majesty's Inspectorate of Constabulary, *Review of the Lessons Learned from the Metropolitan Police Service's Investigation of Home Office Leaks* (2009), para 9.3.

5.9 **We provisionally conclude that improvements could be made to the Protocol. Do consultees agree? [5.20]**

5.10 We provisionally suggest two ways in which we think the Protocol could be improved. First, by adding a definition to the term “serious offence” so it is clear as to the types of conduct to which it relates. This would clarify when it is necessary to invoke the Protocol. Secondly, by introducing greater involvement of legal advisors earlier in the process. This would ensure that the risk of the information being further disseminated is minimised, whilst maximising the potential for any evidence subsequently to be admissible in a criminal trial. This would also ensure that other offences that may have been committed can be identified. We appreciate, however, that if sensitive information is disclosed, a decision may be taken to maximise the chances of the information being swiftly retrieved.

5.11 **Do consultees have a view on whether defining the term “serious offence” and ensuring earlier legal involvement would make the Protocol more effective? [5.24]**

5.12 **Do consultees have other views on how the Protocol could be improved? [5.25]**

The trial process

5.13 A trial for an Official Secrets Act offence will involve information that potentially relates to national security and is therefore of an extremely sensitive nature. The Official Secrets Act 1920 reflects these sensitivities by allowing the judge to exclude members of the public from the court during the proceedings if the Crown provides sworn evidence that disclosure would "be prejudicial to the national safety”.

5.14 Open justice is a fundamental principle to the rule of law and democratic accountability. This has long been recognised by the courts. There is currently uncertainty surrounding whether the power conferred upon the court by section 8(4) of the Official Secrets Act 1920 is aligned with how other provisions that empower a court to hold hearings in private are applied. These other provisions grant the court the power to exclude the public only if it is necessary to do so.

5.15 To reflect the fundamental nature of the principle of open justice, we provisionally conclude that this power be subject to a test of necessity.

5.16 **The power conferred on the court by section 8(4) of the Official Secrets Act 1920 ought to be made subject to a strict “necessity” test whereby members of the public can only be excluded if necessary to ensure national safety (rather than the weaker term used in the 1920 Act ”prejudice”). Do consultees agree? [5.41]**

Authorised jury checks

5.17 Section 118 of the Criminal Justice Act 1988 abolished the right of the defence to challenge jurors without cause.[22] The right of the prosecution to do so is limited to those cases which involve national security or terrorism.[23] 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.[24] The guidelines make clear that the authority to use this power must be personally authorised by the Attorney General, on the application of the Director of Public Prosecutions.

5.18 Given the nature of cases involving terrorism and cases that touch upon national security, we believe this process continues to fulfil an important role in the context of the Official Secrets Acts. In addition, our initial fact finding with stakeholders has not suggested that this process gives rise to problems in practice. Admittedly this is difficult to assess given the fact prosecutions for offences contrary to the Official Secrets Acts are so rare. We do, however, believe the guidance ought to be amended by making clear that if authorised jury checks have been undertaken, that this is brought to the attention of the defence.

5.19 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.

5.20 **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? [5.48]**

Issues that apply generally to criminal trials in which sensitive information may be disclosed.

5.21 Although our consultation paper focuses principally on the narrow issues in the context of a trial involving the Official Secrets Acts, we are mindful that these issues could arise in the context of any criminal trial that involves the disclosure of information that relates to national security

5.22 Our analysis reveals a sharp contrast between the powers possessed by the court in the context of criminal proceedings, which derive largely from the common law and the Contempt of Court Act 1981, and civil proceedings. In the civil context there have been a number of relatively recent legal developments. One such development is Part 2 of the Justice and Security Act 2013 which provides for what is called “Closed Material Procedure”. This procedure permits courts to consider any material which would be “damaging to the interests of national security” if disclosed, without such material being disclosed to the non-Governmental party to the case.

[22] J Gobert, “The peremptory challenge - an obituary” (1989) *Criminal Law Review* 528.

[23] Governed by *Criminal Procedure Rules* (2016), rule 25.8(3). Discussed in D Ormerod and D Perry (eds), *Blackstone’s Criminal Practice* (2017), at D13.22 – D13.45.

[24] For early analysis, see A Nicol, “'Official Secrets and Jury Vetting” (1978) *Criminal Law Review* 284.

5.23 In contrast to the civil law, the criminal law still relies upon the common law and legislation not necessarily intended to reconcile the competing interests at hand. Although not strictly within our terms of reference, we have provisionally concluded it is worth undertaking 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 with the right to a fair trial and the principle of open justice.

5.24 **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? [5.60]**

CHAPTER 6 - FREEDOM OF EXPRESSION

6.1 In this chapter of our consultation paper we consider the extent to which offences that criminalise the unauthorised disclosure of information impact upon the fundamental right to freedom of expression. In doing so, we first examine how the right to freedom of expression has been interpreted by both domestic courts and the European Court of Human Rights and then examine general principles, bearing in mind that freedom of expression is not an absolute right. We explore in detail the approach that is taken when the courts are considering whether a provision that infringes freedom of expression violates the European Convention on Human Rights.

6.2 The right to freedom of expression is not absolute. An interference with the right to freedom of expression will comply with the European Convention on Human Rights provided all of the following criteria are satisfied. These criteria are set out in Article 10(2) of the European Convention on Human Rights:

(1) The interference was prescribed by law.

(2) The interference sought to pursue one of the legitimate aims listed in Article 10(2).

(3) The interference was necessary in a democratic society.

6.3 In the context of the Official Secrets Act 1989, the relevant legitimate aim would be "the interests of national security" which is explicitly included in Article 10(2). The most difficult aspect of considering whether any infringement of the right to freedom of speech complies with Article 10 is the question of whether the measure was necessary in a democratic society. This incorporates a test of proportionality.

6.4 In examining the domestic case law we analyse the House of Lords' decision in *Shayler*, in which the House of Lords rejected the argument that the offences contained in the Official Secrets Act 1989 violated Article 10. The House of Lords placed emphasis upon the fact the Official Secrets Act 1989 does not contain a blanket prohibition on the disclosure of certain categories of information. An offence is only committed if the disclosure was made without lawful authority.

6.5 If authorisation were to be refused, Lord Bingham stated that the individual in question could seek judicial review of this decision. Given that the decision to refuse authorisation impacts upon a right enshrined in the European Convention on Human Rights, Lord Bingham stated that any such refusal must be subject to rigorous scrutiny. For this reason, Lord Bingham rejected the argument that judicial review offered insufficient protection for individuals in the appellant's position. The other Law Lords agreed with the conclusion of Lord Bingham.

6.6 There is more recent case law of the European Court of Human Rights in which it has considered the extent to which provisions that prohibit those who work in the public sector from disclosing information comply with Article 10. Nothing in the more recent case law of the European Court of Human Rights, which we assess in detail in our consultation paper, has caused us to reconsider the continuing validity of *Shayler.*

6.7 For example, the European Court of Human Rights in *Guja* did not decide that compliance with Article 10 mandates the creation of a statutory public interest defence.[25] It did state that the public interest in the disclosed information must be considered, but that is not the same thing. In this more recent case law, the court has recognised that public disclosure of the information should be a last resort. In other words, a person should only make a public disclosure once he or she has exhausted the internal routes available for having the grievance addressed.

6.8 **Compliance with Article 10 of the European Convention on Human Rights does not mandate a statutory public interest defence. Do consultees agree? [6.77]**

6.9 We do conclude, however, that the European Court of Human Rights has clearly expressed the need to ensure that a robust process exists that enables concerns about illegality and impropriety to be raised. Such a process is intended to act as a viable alternative to making a public disclosure. Whilst the House of Lords in *Shayler* expressed confidence in the mechanisms currently in place, as we consider in Chapter 7, we believe there are ways they could be improved.

CHAPTER 7 - PUBLIC INTEREST DEFENCE

7.1 The extent to which offences that criminalise the unauthorised disclosure of information ought to include a public interest defence has pervaded discussion of this area of the law for decades.[26] Given our earlier provisional conclusion that the offences currently contained in the Official Secrets Act 1989 ought to be replaced, we believe it is necessary to evaluate how considerations of the public interest could best be incorporated into any new statutory scheme.

[25] *Guja v Moldova* (2011) 53 EHRR 16

[26] By way of example see, S Palmer, "Tightening secrecy law: the Official Secrets Act 1989", [1990] *Public Law* 243; J Griffith, "The Official Secrets Act 1989" [1989] *Journal of Law and Society* 273; A Bailin, "The last Cold War statute" [2008] *Criminal Law Review* 625.

7.2 In cases such as these, the defendant has made an unauthorised disclosure of protected information in contravention of a prohibition, but argues that he or she did so because it was in the public interest for the information to be disclosed. There are, however, a number of ways public interest could be incorporated into a statutory scheme that criminalises the unauthorised disclosure of protected information.

Model 1: A statutory public interest defence

7.3 We believe that there are a number of arguments that could be made to justify the introduction of a statutory public interest defence. These include enhancing the accountability of government by increasing the likelihood that officials will reveal alleged illegality or impropriety and protecting those who make disclosures that they genuinely believe are in the public interest from criminalisation (perhaps irrespective of whether the disclosure was in fact in the public interest).

7.4 We also identify, however, the risk associated with the introduction of a statutory public interest defence. Such a defence poses a number of risks, both to others and to national security. In addition it undermines the relationship between government and the Civil Service and it undermines the principle of legal certainty.

7.5 As a concept "public interest" involves making value judgments that could be considered arbitrary. It also an amorphous concept about which people may reasonably disagree. By way of example, a question arose in Denmark as to whether it was in the public interest to disclose classified intelligence information on the alleged weapons of mass destruction programme in Iraq prior to the invasion that occurred in 2003. This issue arose as a result of unauthorised disclosures made by a Danish intelligence officer. The Eastern High Court of Denmark did not consider that the unauthorised disclosure was made in "the obvious public interest" because it did not reveal any illegal activity or wrongdoing. The Copenhagen City Court, however, ruled otherwise solely on the grounds that there was considerable public interest in knowing the basis for the decision that was taken to involve Denmark in the invasion of Iraq.[27]

7.6 In an attempt to mitigate those risks we discuss in detail in our consultation paper two models for incorporating considerations of the public interest into the statutory regime that criminalises unauthorised disclosures: the statutory commissioner model, and what we term "the Canadian model". We provisionally conclude that the problems associated with the introduction of a statutory public interest defence outweigh the benefits and explain our belief that the public interest can be better served by the introduction of the statutory commissioner model.

[27] For discussion, see H Nasu, "State secrets and national security" (2015) *International and Comparative Law Quarterly* 365, 395.

7.7 The commissioner model would enable an individual who might otherwise feel compelled publicly to disclose protected information (for example, due to concerns about illegality or impropriety) to bring this concern to the attention of a statutory commissioner independent of his or her organisation. This commissioner would have statutory powers to investigate the allegation and a statutory obligation would be placed upon the relevant parties to assist the investigation. The commissioner would also have an obligation to report to government, subject to the need to ensure information relating to national security is not disclosed. This model would ensure that the public interest in ensuring allegations of impropriety or illegality are investigated. The details of this model are discussed in greater detail below.

7.8 **The problems associated with the introduction of a statutory public interest defence outweigh the benefits. Do consultees agree? [7.66]**

Model 2: The statutory commissioner model

7.9 Although we have provisionally concluded that the case has not been made for the introduction of a statutory public interest defence, we believe a statutory commissioner model would ensure alleged illegality or impropriety can brought to light without the problems associated with such a defence.

7.10 In suggesting that model we examine in detail the extent to which such processes exist within the current law and evaluate whether improvements could be made. In doing so, it is necessary to draw a distinction between Crown servants generally and members of the security and intelligence agencies.

The position of civil servants generally

7.11 All civil servants are bound by the Civil Service Code, which advises those with concerns about alleged illegality or impropriety to raise them within their line management chain, or one of the department's nominated officers, and report any criminal activity to the police or regulatory authorities.

7.12 If a civil servant is not satisfied with the response he or she receives after following this process, he or she may report the matter in question to the Civil Service Commission which has statutory powers that enable it to investigate complaints. Although it is used infrequently, something which is perhaps attributable to its own guidance, a process does exist that enables concerns from civil servants to be investigated by independent statutory commissioners. We believe that this satisfies the public interest as it means allegations of impropriety can be investigated and ultimately resolved.

7.13 **We welcome views from consultees on the effectiveness of the Civil Service Commission as a mechanism for receiving unauthorised disclosures. [7.84]**

Members of the security and intelligence agencies

7.14 Given the sensitive nature of their work, a different regime operates for members of the security and intelligence agencies who wish to raise a concern that relates to their employment. As the House of Lords in *Shayler* explained, there is a list of officeholders who can be approached directly with any concerns, such as the Attorney General and the Commissioner of the Metropolitan Police Service.[28]

7.15 In addition to these officeholders, there are a number of processes which exist and which are available to a member of the security and intelligence agencies who has concerns relating to his or her work.

7.16 First, as the Intelligence and Security Committee noted in its 2007-2008 Annual Report, in 2006 the Security Service established the post of "Ethical Counsellor". Our initial fact finding confirmed that each of the security and intelligence agencies has its own Ethical Counsellor.

7.17 Secondly, if the individual in question wishes to raise the matter with someone who is independent of the agency in question, then he or she can contact the Staff Counsellor, a post fulfilled by someone who is not a member of any of the security and intelligence agencies. Stakeholders have told us that this is perceived to be a relatively informal means of addressing concerns through dialogue and explanation.

7.18 Although we are confident that the role performed by the Staff Counsellor is valuable and ought to be retained, we nevertheless believe it is necessary to evaluate whether more formal means ought to exist that would enable a member of the security and intelligence agencies to bring a concern relating to his or her work to the attention of a statutory officeholder who is independent of the agency in question, and who has the power to investigate and report on the allegations, adding an additional, external tier to the regime that is currently in operation.

Options for the introduction of a statutory post

7.19 Our consultation paper goes on to evaluate two options for adding an additional, external tier to the existing regime.

7.20 We consider the less suitable option would be to enshrine in legislation the mechanism that already exists, namely the Staff Counsellor. Although this could provide an opportunity to clarify the nature of the role played by the Staff Counsellor, and bring a greater degree of transparency to the appointment process, we are concerned it could undermine the Staff Counsellor's role as an informal, independent mediator who achieves the resolution of issues by way of dialogue and explanation.

[28] *R v Shayler* [2002] UKHL 11; [2003] 1 AC 247, para 27. The Attorney General and the Commissioner of the Metropolitan Police Service are included as persons to whom authorised disclosures can be made in the Official Secrets Act (Prescription Order) 1990, SI 1990/200.

7.21 A second option is to retain the post of Staff Counsellor and establish a statutory commissioner who could receive and investigate concerns from members of the security and intelligence agencies. These posts would be complementary in the sense that the Staff Counsellor would continue to act as a more informal mediator whilst the statutory commissioner would be available if a member of staff wished to invoke a more formal process.

7.22 We discuss whether the scheme recently incorporated in the Investigatory Powers Act 2016 provides a solution to this new appointment and conclude that it does. That Act introduces the role of the Investigatory Powers Commissioner. This office will have the following characteristics:

(1) The Commissioner currently holds or has held high judicial office.

(2) A person does not commit an offence for disclosing information to the Commissioner.

(3) The Commissioner is appointed under statutory powers.

(4) The Commissioner acts independently of the agencies.

(5) If an investigation is initiated there is a statutory obligation to assist this investigation.

(6) The Commissioner must report annually to the Prime Minister who must lay the report before Parliament, ensuring there can be scrutiny of the work that is undertaken.

7.23 We believe that the introduction of the Investigatory Powers Commissioner, supported by the Judicial Commissioners, would provide a suitable means of ensuring that members of the security and intelligence agencies have an additional option available to them should they wish to raise a concern relating to their work in a more formal setting with an officeholder who is independent of the agency in question. That this is a function the Commissioner fulfils ought to be made clear.

Conclusion on the statutory commissioner model

7.24 Our consultation paper concludes that the position of Staff Counsellor ought to be retained, but that it ought to be supplemented by the Investigatory Powers Commissioner. This would mean that a member of the security and intelligence agencies harbouring concerns relating to his or her work would have the option of not only disclosing this concern internally to the Ethical Counsellor, but also externally to the Staff Counsellor and, if he or she were still not satisfied, then the issue could be brought to the attention of the Investigatory Powers Commissioner.

7.25 We agree with Liberty and Article 19 who concluded in a joint report that:

> Relying on whistleblowing to expose wrongdoing is unsatisfactory and a poor substitute for properly effective structures of accountability, both internal and external.[29]

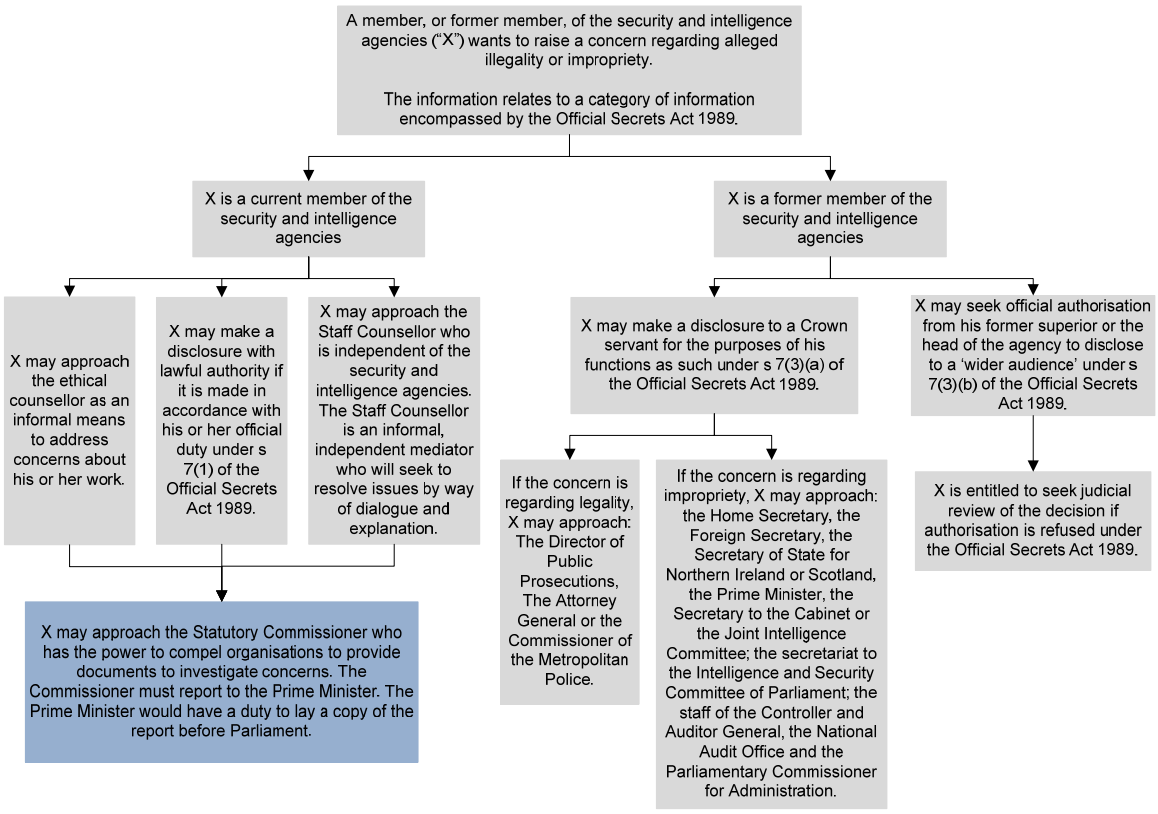
[29] Liberty and Article 19, Secrets, Spies and Whistleblowers: Freedom of Expression in the UK (2000), para 7.3.

7.26 The ability to disclose information to a statutory Commissioner would provide an additional level of external accountability.

7.27 **A member of the security and intelligence agencies ought to be able to bring a concern that relates to their employment to the attention of the Investigatory Powers Commissioner, who would be able to investigate the matter and report their findings to the Prime Minister. Do consultees agree? [7.119]**

7.28 The Staff Counsellor is available to be consulted by staff in other departments closely involved in intelligence work provided that the issue he or she wishes to discuss relates to his or her access to intelligence.[30] We envisage the Investigatory Powers Commissioner being available to receive concerns from members of staff in these departments in addition to those working in the security and intelligence agencies.

7.29 Below we have produced a diagram to illustrate how the statutory commissioner model would fit within the existing framework.



7.30 As can be seen, the statutory commissioner model provides an additional avenue by which to raise concerns and ensures:

(1) Information that may cause damage if it were to be disclosed is protected.

[30] This was confirmed by the Prime Minister in a written statement to the House of Commons. See Hansard, House of Commons, 21 April 2016, HCWS694, col 27WS – 28WS.

(2) Greater accountability is achieved by the power of the statutory Commissioner to investigate matters that are brought to his or her attention. This is augmented by the existence of a statutory obligation to assist any investigation carried out by the commissioner. A degree of transparency is ensured by the obligation to lay a report detailing the work of the statutory commissioners before Parliament.

Model 3: The "Canadian model"

7.31 We also discuss a third model adopted in Canada but as yet untested in reported cases. In Canadian law, the Security of Information Act 2001 makes it a criminal offence for anyone permanently bound to secrecy from communicating or confirming "special operational information". Such an individual does not commit an offence under the Act if his or her purpose is to:

> Disclose an offence under an Act of Parliament that he or she reasonably believes has been, is being, or is about to be committed by another person in the purported performance of that person's duties and functions for, or on behalf of, the Government of Canada.

7.32 In addition, the public interest in disclosure of the information must outweigh the public interest in non-disclosure. The Canadian legislation enumerates the factors a court must consider when assessing whether the disclosure was in the public interest.

7.33 In our consultation paper we discuss the difficulties of this model, concluding that we did not believe that the Canadian model would bring additional benefits or overcome a number of the problems caused by the introduction of a statutory public interest defence identified above. Furthermore, the model could undermine confidence in the ability of the Investigatory Powers Commissioner to discharge their functions.

7.34 **The Canadian model brings no additional benefits beyond those that would follow from there being a statutory commissioner who could receive and investigate complaints from those working in the security and intelligence agencies. Do consultees agree? [7.131]**

Public disclosures

7.35 The mechanism we have provisionally concluded ought to be introduced would enable a member of the security and intelligence agencies to raise a concern relating to his or her work with an officeholder independent of his or her organisation but would not authorise such an individual to make a public disclosure.

7.36 If a former member of the security and intelligence agencies wishes to make a public disclosure, he or she could seek official authorisation in accordance with section 7(3) of the Official Secrets Act 1989.

7.37 By virtue of section 7(1) of the Official Secrets Act 1989, a disclosure made by a Crown servant, a member of the security and intelligence agencies or notified person is made with lawful authority if, and only if, it is made in accordance with an official duty. On its face, it seems as though there is no mechanism for current members of the security and intelligence agencies to seek authorisation to make a disclosure. Our preliminary fact finding with stakeholders has confirmed, however, that a process for seeking authorisation to make a disclosure is included in the contract of employment of those who are members of the security and intelligence agencies. This process is intended to ensure Article 10 compliance.

7.38 Despite the fact that in practice there is already a process whereby authorisation to make a disclosure can be sought, we believe this is something that ought to be enshrined in legislation. This would, it is hoped, inspire greater confidence in the system and ensure the Article 10 right to freedom of expression is more robustly protected.

7.39 **It should be enshrined in legislation that current Crown servants and current members of the security and intelligence agencies are able to seek authority to make a disclosure. Do consultees agree? [7.139]**

7.40 Despite Lord Bingham's conclusion in *Shayler* that the authorisation process is compliant with Article 10 of the European Convention on Human Rights, we believe there are ways it could be improved. We believe that one way would be to enshrine in statute a non-exhaustive list of factors that ought to be taken into consideration when deciding whether authorisation to make a disclosure ought to be declined. This echoes the view that was taken in *Shayler*, in which Lord Bingham stated that authorisation should only be declined when disclosure of the information in question would be detrimental to national security and/or would cause damage to the work of the security and intelligence agencies.[31]

7.41 A non-exhaustive list would increase the predictability and transparency of the process and would act as an additional safeguard against decisions that do not have sufficient regard for the employee's right to freedom of expression, whilst also dealing with one of the criticisms Lord Hope made of the legislation in *Shayler*.[32]

7.42 **There should be a non-exhaustive list of the factors to be considered when deciding whether to grant lawful authority to make a disclosure. Do consultees agree? [7.142]**

[31] *R v Shayler* [2002] UKHL 11; [2003] 1 AC 247, para 30.

[32] *R v Shayler* [2002] UKHL 11; [2003] 1 AC 247, para 70-85. These are discussed in greater detail in Chapter 6.

A statutory public interest defence for journalistic activity

7.43 Finally, in our consultation paper, we discuss that different considerations may apply in the context of journalistic activity given that the press "plays a vital function in democracy".[33] In his *Inquiry into the Culture, Practices and Ethics of the Press*, Lord Justice Leveson doubted whether journalists ought to be treated differently from other citizens for the purposes of determining whether they have committed criminal offences,[34] adding:

> A press considering itself to be above the law would be a profoundly anti-democratic press, arrogating to itself powers and immunities from accountability which would be incompatible with a free society more generally.[35]

7.44 Lord Justice Leveson later considered two practical issues associated with the introduction of a statutory public interest defence specifically for journalists. First, that such a defence could preclude the commencement of a prosecution even when the activity in question was clearly not in the public interest.

7.45 Secondly, Lord Justice Leveson queried the necessity of introducing a public interest defence specifically for journalists. Given the fact the Director of Public Prosecutions has promulgated guidelines that must be considered when a prosecutor is deciding whether to charge a journalist with a criminal offence, Lord Justice Leveson concluded that sufficient safeguards were already in place.

7.46 For the reasons identified above and given the depth and breadth of analysis in such a recent report, we agree with Lord Justice Leveson's conclusion that journalistic activity is already sufficiently protected by the safeguards that currently exist. In addition, it is our view that the introduction of a statutory public interest defence solely for journalists could be considered arbitrary, given that there are other professionals who might violate the criminal law in the pursuit of their legitimate activities.

7.47 **The legal safeguards that currently exist are sufficient to protect journalistic activity without the need for a statutory public interest defence. Do consultees agree? [7.76]**

[33] B Leveson, *An Inquiry into the Culture, Practices and Ethics of the Press* (2012), Vol 1, Ch 2, para 5.1.

[34] B Leveson, *An Inquiry into the Culture, Practices and Ethics of the Press* (2012), Vol 1, Ch 2, para 5.6.

[35] B Leveson, *An Inquiry into the Culture, Practices and Ethics of the Press* (2012), Vol 1, Ch 2, para 5.6.