Law Commission
Reforming the law

PROTECTION OF OFFICIAL DATA: SUMMARY

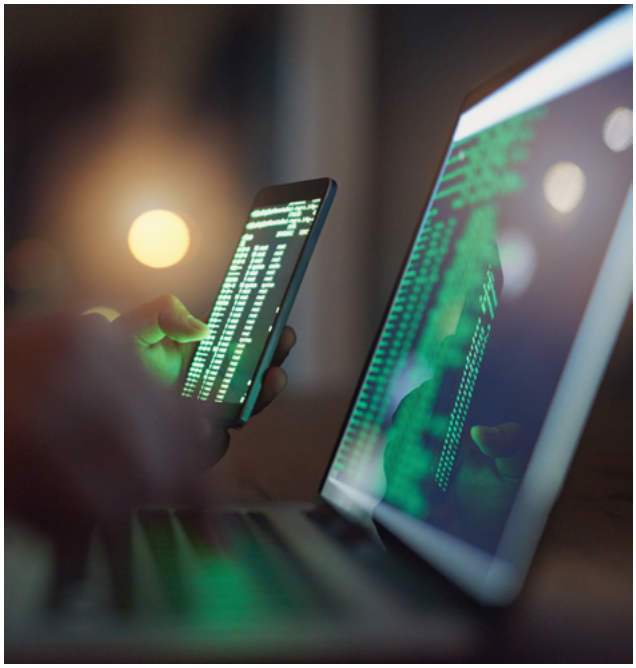
INTRODUCTION

The scale and potential impact of espionage and of unauthorised disclosures ("leaks") 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.**

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.

The criminal law provisions that protect official information are primarily contained in the Official Secrets Acts 1911-1939 and 1989.

The offences in these Acts are outdated and in urgent need of reform.



The purpose of this Report is to recommend much needed reform of these Acts (amongst others). The recommendations are designed to ensure:

i. that the law governing both espionage and unauthorised disclosures addresses the nature and scale of the modern threat;
ii. that the criminal law can respond effectively to illegal activity (by removing unjustifiable barriers to prosecution); and
iii. that the criminal law provisions are proportionate and commensurate with human rights legislation.

The Report

Our Report makes 33 recommendations, some of which we note in this Summary, and makes recommendations in three distinct areas.

- Our first series of recommendations relates to **espionage:** the criminalisation of individuals whose purpose is to gain access to sensitive information. These provisions are currently contained in the Official Secrets Acts 1911, 1920 and 1939.
- Our second series of recommendations relates to the criminalisation of individuals for **disclosing official information without authorisation.** These provisions are primarily contained in the Official Secrets Act 1989 (though there are many other miscellaneous disclosure offences).
- Our third and final series of recommendations relates to disclosures that are in the **public interest.**

Our recommendations are based on independent legal analysis, open consultation and the detailed assessment of evidence. It is, however, a *legal* report. It deals with highly sensitive matters that are both legally and politically complex. There are some important matters that we have considered for which there is no clear, single, 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.

Consultation and Evidence

This Report has benefitted from the insight of a great many consultees (we received over 1,200 responses to our 2017 consultation paper), including those in the media, academia and legal services.

Similarly, we 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.

Some of the evidence on which we have relied is classified as SECRET or TOP SECRET, and so cannot be published. In order to make clear where we have relied on classified evidence, we have published hypothetical examples that illustrate the risks revealed by the classified evidence.

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.

OUR RECOMMENDATIONS

Espionage Offences

"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]

We recommend that a new espionage statute – containing modern language and updated provisions – should replace the Official Secrets Acts 1911, 1920 and 1939.

Recommendation 1

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.

The new offences we recommend modernise many aspects of the current offences, as well as remove redundant provisions.

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

We retain, however, the two types of espionage offence:

i. espionage by trespass or observation; and

ii. espionage by collection and communication of information.

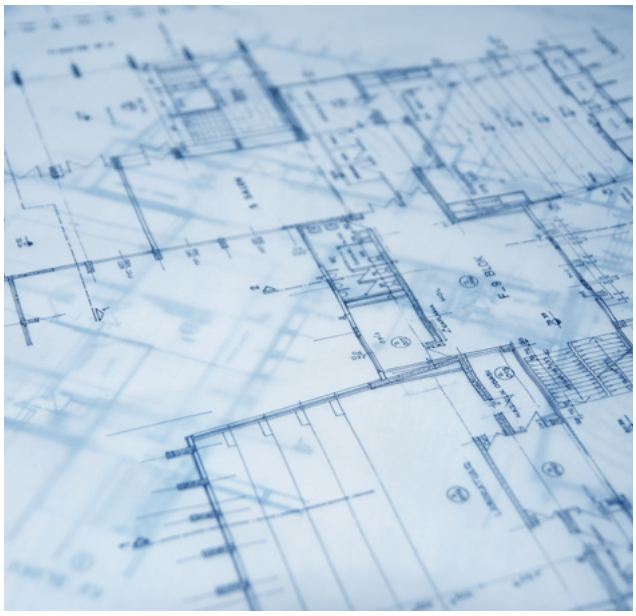
Recommendation 7

We note some of our key recommendations here.

Archaic language

"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."

Para 3.88 of the Report



The 1911 and 1920 Acts contain references to "a sketch, plan, model, note and secret official pass word and code word", which we consider are anachronistic and not reflective of the types of information needing protection.

These terms should be replaced with "document, information or other article". Information should be defined to include any program or data held in electronic form.

Recommendation 7

Replacing "enemy" with "foreign power"

Sections 1(1)(b) and 1(1)(c) of the Official Secrets Act 1911 provide that it is an offence for a person to make or obtain "any sketch… 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*".

We are concerned that, 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.

We are equally concerned that any replacement for the term "enemy" should not render the offence overly-broad.

We therefore recommend that, in any new statute to replace the OSA 1911, "enemy" be replaced with "foreign power".

Recommendation 2

This is subject to that term being sufficiently tightly defined. It should be defined to ensure it includes not only foreign governments and those purporting to exercise or assume the role of governments outside UK territory, but also those engaged in **terrorism and entities directed and controlled by a foreign government.**

Extraterritoriality

Section 10 of the OSA 1911 provides that the offences contained in that Act can only 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.

This definition is excessively restrictive. Many people may have access to British assets located outside the UK, albeit that they are not themselves a British Officer or subject (such as local embassy staff).

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.

Further, "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).

Recommendation 10

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 [official data overseas] 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."

Para 3.143 of the Report

Failing to define "significant link" in such a way would weaken the effect of many of our other recommended reforms to espionage legislation.

Unauthorised Disclosure Offences

This part addresses unauthorised disclosure offences, primarily under the Official Secrets Act 1989. We therefore recommend that the OSA 1989 be reformed.

The OSA 1989 contains a number of different offences applying to certain categories of information:

- information relating to security or intelligence (s1);
- defence (s2);
- international relations (s3);
- crime and special investigation powers (s4);
- information resulting from unauthorised disclosures or entrusted in confidence (s5); and
- information entrusted in confidence to other states or international organisations (s6).

The offences in sections 1 to 4 can only be committed by Crown servants or government contractors – or, in the case of section 1(1), those notified that they are subject to its provisions.

The offences in sections 5 and 6 can be committed by anyone.

We make many recommendations in this part, some substantive and some procedural. The following are of particular note.

Requirement to prove damage

We recommend that the offences in sections 1(3)-4 of the OSA 1989 (which apply only to Crown servants and government contractors) **should not continue to require proof of damage.** Instead, the offences should require an **explicit fault element.**

Recommendation 11

By "fault element" we mean, for example, proof of the defendant's knowledge or belief that the disclosure would cause damage – although we have not recommended a particular fault element.

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.

These recommendations ensure both that prosecutions are not unjustly hampered by the need to disclose further secret material in open court, and also that the offences reflect a sufficient degree of culpability.

Further, as explained below, 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.

Legal advice

There is a persuasive argument that, in some cases, disclosures for the purpose of legal advice should be authorised. However, such disclosures should not risk the security of highly sensitive information: it is only as secure as the weakest link the chain. Highly sophisticated actors across the globe will attempt to exploit any weakness (whether personal or technical) in the protection of sensitive information. Safeguards must be in place.

We 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.

Recommendations 15-17

Maximum sentences

The scope for damage following an unauthorised disclosure is now many times greater than at any point in the past. A disclosure is not limited to the number of hard-copy documents that can physically be removed and disclosed. Terabytes of data can now be disclosed in a single act of disclosure, with far-reaching consequences.

"A single unauthorised disclosure… could result in serious harm or perhaps even death."

Para 5.45 of the Report

Nonetheless, the maximum sentence for an offence under the OSA 1989 is two years, which does not reflect the culpability of an individual in the most egregious cases.

We therefore recommend that Parliament should consider increased maximum sentences for some offences under the Official Secrets Act 1989, as well as 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.

Recommendation 14

Whilst we are recommending a review of the maximum sentence, we do not recommend any particular sentence; this is for Parliament to determine. There would also be scope for considering whether different maximum sentences should apply to the offences in sections 1-4 as against those in sections 5 and 6.

Extraterritoriality

Currently, by virtue of section 15(1) of the OSA 1989, 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 are concerned to ensure that the offence applies equally to government contractors and notified persons (whether or not they are British citizens) as it does to British citizens and Crown servants.

We therefore recommend that 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.

Recommendation 21

Public Interest Disclosures

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 European Convention on Human Rights ("ECHR"), concerning the right to freedom of expression.

"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."

Para 1.34 of the Report

The right to freedom of expression is not absolute 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.

The State has a broader discretion to interfere with the Article 10 rights of public servants (who owe a duty of "loyalty, reserve and discretion") than it does when interfering with the rights of civilians (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.

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.

Civilians

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:

1. first, whether the subject matter of the disclosure was in the public interest; and,
2. secondly, whether the manner of disclosure was in the public interest.

We also explain our view that, as with a few defences in criminal law, 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"), because we regard this as a political matter for Government and, ultimately, Parliament to determine in any legislation.

Public servants

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.**

We therefore recommend that 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.

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.

Recommendation 32

We also recommend that 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.

Recommendation 33

The full Report can be viewed at https://www.lawcom.gov.uk/project/protection-of-official-data/

QUESTIONS AND ANSWERS

Q: What offences are you recommending?

A: We are recommending that the Official Secrets Acts 1911, 1920 and 1939 be replaced with a new Espionage Act, but the new Act should retain the two existing types of espionage offence (espionage by trespass or observation and espionage by collection or communication of information). We are not recommending replacement of the Official Secrets Act 1989 (concerned with unauthorised disclosures, or "leaks"), but we are recommending reform of those existing offences.

Q: Would the public interest defence apply to both the new Espionage Act and the Official Secrets Act 1989?

A: No. To be guilty of espionage, an individual would have to act with a purpose they knew or had reasonable cause to believe was prejudicial to the interests of the state. This is not commensurate with a public interest defence. The defence would only be available to those charged with an offence under the OSA 1989.

Q: What determines the "public interest"?

A: This is essentially a political issue. We therefore come to no conclusion on this point and leave it to Parliament to determine. However, we do note that, at a minimum, asking whether a disclosure was in the public interest would involve considering not just whether the subject matter of the disclosure was in the public interest, but whether the manner of that disclosure was in the public interest.

Q: What do you mean by "whether the manner of disclosure was in the public interest"?

A: Whether a disclosure was in the public interest is not just a question of whether the subject-matter of some information in that disclosure happened to be in the public interest. A full assessment of whether the disclosure served the public interest will consider whether, for example, the disclosure was more damaging than necessary (because, say, there were thousands of other documents disclosed that were not in the public interest). There is also a public interest in civil servants being loyal to the democratically elected government, whereas the public interest in journalism lies in the government being held to account, so different considerations will have to be weighed in the balance when assessing the public interest. The final details of the defence are, however, a matter for Parliament.

Q: There are lots of avenues for reporting concerns of wrongdoing; why do you need a new statutory commissioner?

A: While it is true that there are a number of avenues for disclosing these concerns (including the Metropolitan Police, the Intelligence and Security Committee of Parliament, as well as internal routes), we are concerned that they will not in all cases constitute an effective investigative mechanism for the purposes of Article 10 ECHR. Public servants should have confidence that their concerns will be investigated by a body that is free of the potential for improper influence and that is able to investigate expeditiously. It is too simplistic to say that, *taken together*, the existing avenues for reporting concerns constitute an effective investigative mechanism: in cases of urgency, to how many different bodies should a public servant be expected to report concerns before it is clear that an investigation is under way? An independent statutory commissioner with investigatory powers and expertise would afford a clear and effective avenue for reporting concerns.

Q: Will your recommended changes to extraterritoriality significantly broaden the scope of the offences?

A: The recommendations are not about simply broadening the scope of the offences, but ensuring that the offences are able to address the nature of modern espionage (in the case of our espionage recommendations) and ensuring that public servants who would be guilty of a disclosure offence when in the UK are not free to disclose information without authorisation merely because they are abroad.

Q: Why should lawyers giving legal advice be vetted before they can receive disclosures? Surely lawyers are reliable?

A: We want to ensure that disclosures for the purposes of legal advice can, when necessary, be authorised disclosures, so that lawyers can provide the best advice to their clients, whilst also ensuring that highly sensitive information does not risk falling into the wrong hands. There are highly sophisticated actors across the globe who will employ any means to access classified government data and will exploit any weakness, whether relating to the personal circumstances of the lawyer or, for example, to their IT systems. Our recommendations mitigate that very real risk.

Q: Increasing the maximum sentence seems very draconian, does it not?

A: To be clear, we are not proposing a specific maximum sentence. It is nonetheless apparent that the potential damage that an unauthorised disclosure can cause is orders of magnitude greater than was the case in the last century, and so the current maximum (two years) does not necessarily allow for appropriate punishment of the most serious cases. This does not mean that everyone who is guilty of an offence would receive the maximum sentence or anything necessarily approaching it – this is not how sentencing works. A sentencing regime should reflect the culpability of the defendant.

Q: Will removing the damage requirement in the OSA 1989 offences make it too easy to prosecute someone?

A: No; we are replacing it with a fault element (such as, for example, knowledge or belief that the disclosure would cause damage – although we have not recommended a particular fault element). Our concern was that requiring the prosecution to prove damage flowing from a disclosure would require them to introduce further sensitive information into court, so compounding the original damage. This meant that prosecutions that should have gone ahead, or might need to go ahead in future, could not. However, adding an explicit fault requirement better reflects the culpability of the defendant. The public interest defence also allows the defendant to argue that there was a public interest in the disclosure despite any damage caused.