Introducing a public interest disclosure defence

Briefing Paper

Mishcon de Reya

It's business. But it's personal.
mishcon.com

This Briefing Paper sets out the basis for the introduction of a public interest disclosure defence for breaches of the Official Secrets Acts ("OSAs") or any replacement Espionage Act. The authors of the Paper are a team of lawyers from Matrix Chambers and Mishcon de Reya LLP, who together have experience of prosecuting and defending in Official Secrets Act trials and acting in national security related proceedings. They bring this experience to bear in their support for the introduction of a public interest defence. Their work on this issue is funded by Janus Friis as part of his philanthropic endeavours focussed on supporting accountability and transparency in government

The background

The introduction of a public interest defence is a necessary constituent of any new, fit-for-purpose statutory framework which meets the needs of a modern democracy and protects both national security and the rule of law. The need for a public interest defence has been recognised by the Law Commission in its recent report, *Protection of Official Data* (September 2020), which recommends, following extensive consultation, 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."*

The Law Commission sets out over several hundred pages the basis for that conclusion. This Briefing Paper seeks, by reference to the Law Commission research and other sources, to provide a clear summary of the reasons that a public interest defence should form a crucial part of the UK's renewed Official Secrets/Espionage law.

Alongside their support for the introduction of a public interest defence, the Law Commission also highlighted the need for a comprehensive overhaul of the existing Official Secrets legislation to meet evolving modern needs. Concerns about the aptitude of the OSAs for the modern context have also been expressed by the cross-party Intelligence and Security Committee of Parliament in their Russia report (HC 632, 21 July 2020), which highlighted the inadequacy of the existing legislation in handling the type of data and technology-related threats to national security that now exist. When Parliament responds to this need for new, national security protecting legislation – which, it is anticipated, will form part of this session's legislative agenda – it is critical that a public interest defence also features in the new legislation, to ensure an appropriate balance between the competing public interests engaged in this sphere. The ISC in its report urged Parliament to consider carefully the Law Commission's forthcoming recommendations.

The overarching context

A functioning democracy requires, on the one hand, the power to limit the disclosure and dissemination of information, the publication of which would be harmful to national security; and, on the other hand, a sufficient degree of public scrutiny and transparency to hold the government to account. These indispensable characteristics of a liberal democracy can pull in opposite directions from each other, and an appropriate balance between them needs to be struck. As the Law Commission has observed:

> *"The public interest in national security and the public interest in transparent, accountable government are often in conflict. While, no doubt, public accountability can ensure that government is protecting national security, the relationship between security and accountability is nonetheless one of tension. Effective protection of our national security relies on laws of confidence and secrecy. Used well, these laws protect our democracy, our economic well-being, and our lives; we sacrifice a portion of our liberties in order to ensure that we have any liberties worth sacrificing. Abused, these laws allow wrongdoing to flourish – for states to place themselves beyond the reach of the law – and so undermine the very democracy their creation sought to uphold."*

The law, and society's expectations, have moved on immeasurably since the First World War and Cold War eras when the OSAs were enacted. Sir Humphrey Appleby of 'Yes Minister' famously quipped "Open government is a contradiction in terms. You can be open or you can have government." But the serious point is that freedom of information was undoubtedly a nascent and novel concept in former times, yet is now accepted as a basic tenet of any accountable democracy. Professor Jacob Rowbottam, in his response to the Law Commission consultation, provided an elegant summary of the basic position which has now evolved:

> *"Everyone accepts that some government information must remain secret. The system of secrecy, however, requires safeguards to ensure that the power to withhold information is not abused to shield government from criticism or embarrassment, or to cover up wrongdoing."*

If, as is anticipated, the existing Official Secrets legislation is updated by way of an Espionage Act which strengthens the protection of national security, the new legislative framework must also contain provisions that strengthen accountability in order to maintain the delicate balance of rights on which democracy depends. A public interest defence is an essential part of that balance.

Indeed, even if a new Espionage Act is not introduced, there is a strong rationale for amending the existing OSAs to introduce a public interest defence. As the Law Commission has underscored, the absence of such a defence in the current statutory framework raises real questions about whether the balance is currently struck in a way that complies with the UK's legal obligations, in particular its obligations to protect freedom of expression. Furthermore, the absence of any public interest defence at present puts the UK in the minority among Five Eyes: Australia, Canada and New Zealand have all recognised the need for and introduced some form of the public interest defence into their own domestic law.

What is a public interest defence?

Disclosure of information which is protected by the OSAs, or disclosure by a person subject to the OSAs, is in most circumstances a criminal offence. This means that it will generally be a criminal offence for a Crown servant or other government employee to disclose information obtained in the course of their employment, such as information about the Government's military and intelligence

activities, in particular. It will also be an offence for a journalist or news organisation to publish information which is protected by the OSAs. A public interest defence would operate to remove criminal liability for such a disclosure if the disclosure was objectively in the public interest. It could be relied on both by the individual making the initial disclosure (e.g. a member of the intelligence services) and by anyone who subsequently published the disclosure (e.g. journalists).

Generally, a public interest defence requires an individual to demonstrate both an objective and subjective element (or, in some cases, one of the two), in order to benefit from the defence. The subjective limb is that the person making the disclosure reasonably believed the disclosure to be in the public interest; the objective limb is that the disclosure actually was in the public interest. The Law Commission's proposal is for a public interest defence that only takes account of whether the disclosure was in fact in the public interest (i.e. that undertakes an objective but not a subjective assessment of the public interest in the disclosure), and that renders irrelevant to the application of the defence a person's own motivation for making the disclosure.

Of course, whether a subjective or objective test is used – or a combination of the two – it will be for the CPS in the first instance to assess whether the disclosure satisfies the public interest test before deciding whether to bring a prosecution, and it will be for the jury at trial to decide whether a defendant's disclosure does in fact satisfy the public interest test releasing them from criminal liability. As the Law Commission have summarised:

> *"A public interest defence would allow a defendant to justify their unauthorised disclosure on the broad basis that disclosure of the information was in the public interest. In the event that the jury agreed, the defendant would not be guilty of the offence."*

At present, the only defences to the OSAs are contrived and already involve the public interest creeping in by the backdoor. For OSA offences in which damage must be proved, it is a defence for the accused to show that s/he did not know and had no reason to believe that the disclosure was damaging or likely to be. This can result in bizarre, *Spycatcher*-type arguments, where the defence may point to prior publication of the substance of the disclosure, which is not itself a defence but may establish that no harm was done by the revelation. But this type of argument is not available to those, such as intelligence officers, prosecuted under section 1, which is an offence of strict liability i.e. there is no requirement to prove any damage. The other main defence is necessity (a defence to all crimes except murder). This is a crude form of public interest where the defendant can establish that the offence of disclosure involved a lesser harm than the crime it sought to prevent. The defence was famously run in the Katharine Gun prosecution (told in the recent *Official Secrets* film) when the former GCHQ employee revealed US attempts to seek UK help in bugging the UN in the crucial vote on the Iraq War, which she contended was unlawful in international law.

The proposed defence

The proposed defence would apply in relation to all offences arising under the current sections 1-6 of the OSA 1989, or to any successor legislation replacing, replicating or enlarging those offences.

Section 1 OSA 1989 applies to members of the security and intelligence services, and to Crown servants, government contractors, and anyone else notified under s.1(1) that the provisions apply to them. It creates an absolute (strict liability) offence of disclosing without lawful authority any information, document or other article relating to security or intelligence which is or has been in the individual's possession by virtue of their position in the security and intelligence services.
Section 2 OSA 1989 creates a similar offence in relation to Crown servants or governments contractors who make damaging disclosures of any information, document or other article relating to defence which is or has been in the individual's possession by virtue of their position as a Crown servant or contractor. A disclosure for the purposes of section 2 is damaging if "it damages the capability of, or of any part of, the armed forces of the Crown to carry out their tasks or leads to loss of life or injury to members of those forces or serious damage to equipment or installations of those forces", or "endangers the interests of the United Kingdom abroad, seriously obstructs the promotion or protection by the United Kingdom of those interests or endangers the safety of British citizens abroad", or is likely to have those effects.

Section 3 creates a similar offence where the information relates to international relations or to an international organisation and section 4 creates an offence where the disclosure results in the commission of a criminal offence, facilitates an escape from legal custody, impedes the prevention or detection of offences or is likely to produce those effects.

The section 1-4 offences apply to specific categories of persons (i) in government employment or under contract with the government or (ii) personally notified under s.1 of the Act. Sections 5 and 6 create offences arising from the use of unauthorised disclosures and therefore apply to the general public and, for example, journalists who publish or pass on material or information that has been leaked to them.

There are strong public interest reasons for the criminalisation of the conduct which falls within sections 1-6 OSA 1989. There are, however, equally strong reasons in the public interest for such unauthorised disclosures, on occasion, to be made – for example where there is serious wrongdoing on the part of the government or individuals working for the government, or concealment of such wrongdoing. In such circumstances, the individual(s) casting light on that misconduct by making an unauthorised disclosure ought to benefit from a public interest defence, otherwise the personal cost of making any such disclosure is likely to be too high for Crown servants and journalists to counter making them, and official misconduct – with all the negative effects for democracy that that entails - will be unlikely to be unearthed.

A public interest defence should, therefore, apply in relation to all of the offences currently contained in sections 1-6 OSA 1989. While the Law Commission preferred not to publish a suggested draft of the defence, contending that such matters are for the legislature, it might provide broadly as follows:

> *In any proceedings for an offence under s.1-6 Official Secrets Act 1989 [or the corresponding provisions of the Espionage Act 2020] it shall be a defence for the accused to prove (i) that the disclosure in question was in the public interest and (ii) the manner of the disclosure was also in the public interest.*

In assessing whether the disclosure was in the public interest the following (non-exhaustive matters) shall be taken into account:

- the subject matter of the disclosure;
- the seriousness of the conduct exposed;
- the harm caused by the disclosure.

In assessing whether the manner of the disclosure was in the public interest the following (non-exhaustive matters) shall be taken into account:

- whether the disclosure is made in good faith.
- whether the extent of the disclosure is no more than reasonably necessary for the purposes of exposing the relevant conduct;
- whether the individual reasonably believes that the information disclosed, and any allegation contained in it, are substantially true;
- whether the disclosure is made for purposes of personal gain;
- the availability of any other effective authorised procedures for making the disclosure and whether those procedures were exercised;
- whether, in all the circumstances of the case, it is reasonable for the disclosure to have been made in the relevant manner.

The need for such a defence is discussed in more detail below, along with the precedents for such a defence which exist both in other UK statutory contexts, in the UK's international legal obligations, and in other jurisdictions.

The problems with the status quo

The problems with the existing Official Secrets legislation arise in two respects: first, it does not sufficiently protect national security because it is outdated and therefore does not adequately respond to the modern and technological context in which risks arise (this was the concern raised by the ISC in its Russia report); and second, because it fails to protect the ability to make disclosures in the public interest and thus fails to ensure a sufficient degree of accountability in government (this is the lacuna that would be remedied by the introduction of a public interest defence).

If, therefore, Parliament considers that the balance needs to swing in favour of protecting national security, concomitant with any steps taken to achieve that (and this Paper does not purport to suggest how that should be achieved), there must be associated augmentations of the protection given to transparency in the public interest. Underscoring the need for this – by way of the introduction of a public interest defence – is the Law Commission's analysis that the status quo under the OSA may already breach the United Kingdom's international law obligations, implemented through the Human Rights Act 1998. That violation would become all the more acute if the balance swung towards protecting national security further without providing the protection of a public interest disclosure defence.

The Law Commission report observes that "we cannot be certain that the current legislative scheme, in the OSA 1989" – which does not provide for a public interest defence – "affords adequate protection to Article 10 rights under the ECHR". Article 10 protects freedom of expression and equivalent protections are also to be found in the domestic common law: *Kennedy v Information Commissioner* [2015] AC 455 para. 46. The Law Commission reached its conclusion following careful analysis of the case law of the European Court of Human Rights and of the House of Lords in *R v Shayler* [2003] 1 AC 247. The *Shayler* case related to the criminal prosecution, under sections 1 and 4 OSA 1989, of a former security services employee who had disclosed documents to the media. It was argued on his behalf that a public interest defence ought to be read into UK law, and that such a defence was necessary for compliance with Article 10 of the European Convention of Human Rights. The House of Lords decided against Mr Shayler but, as the Law Commission report explains in detail, it is very likely that given the evolution of the law over the last 18 years, it is unlikely that the case would be decided in the same way today, and there is a real risk that the failure to provide a statutory public interest defence does now put the UK in breach of its other legal obligations.

Alongside the introduction of a public interest defence, the Law Commission also recommends the establishment of an independent statutory commission to investigate evidence of serious wrongdoing, to whom disclosures could, in the first instance, be made by Crown servants. This is a somewhat novel concept but one worthy of serious consideration. However, the Law Commission recognises that even an independent statutory commission will not always be enough to balance the important constitutional rights at stake, and that therefore the introduction of a public interest defence is an indispensable part of rectifying the problems with the current framework:

> *"There will be exceptional cases in which the disclosure is made by a Crown Servant or other official caught by the OSA 1989 when the commission cannot provide an effective response (e.g. through pressure of time or because it is itself conflicted). Such a commission would also not operate effectively in the case of a journalist or other citizen who is in possession of material protected by the OSA 1989. We therefore also recommend a public interest defence which would be available to those charged with offences under the OSA 1989."*

The Law Commission gives a practical example of a case in which a public interest defence may have made a real difference to the public's awareness of misconduct and to the accountability of public officials for that misconduct. In June 2018, the ISC published a report on *Detainee Mistreatment and Rendition*, 2001-2010. The report concluded that, while there was no evidence to suggest that UK personnel were directly involved in the mistreatment of detainees, there was evidence to suggest that UK personnel were implicated in the mistreatment of detainees carried out by others. By the time of publication, between 8 and 17 years had passed since the conduct assessed. But if there had been a public interest defence, it may well have been that individuals who were aware of this conduct, and of UK personnel's culpability for it, would have felt able to bring it to light much earlier and thus achieved a more meaningful and contemporaneous public oversight, scrutiny and accountability. At present, the law does not provide for any public interest defence even for those who make revelations about the kind of grave mistreatment which emerged in the Baha Mousa Inquiry –indeed an OSA prosecution could be mounted against such whistleblowers on the basis that leaks could spark a backlash against British soldiers. It is difficult to see how our current law is consistent with our obligations to prevent torture occurring anywhere in the world if we criminalise revelation of it in this way without any safety valve.

There are many other examples in which a public interest defence should have been available to the defence. Clive Ponting, the distinguished civil servant who made disclosures concerning the Government's misstatements about the General Belgrano incident in the Falklands war, was acquitted by a jury who ignored the trial judge's directions and clearly felt he had acted in the public interest. Katharine Gun's case, in which she had raised a defence of necessity, was dropped at the door of the Old Bailey when the CPS contended that it could not rebut that defence. Derek Pasquill was prosecuted under section 3 for leaking documents about secret CIA rendition flights and contact with Muslim groups. One document included a warning from the Foreign Office that the Iraq war and UK foreign policy were fuelling Muslim extremism in Britain. His case was belatedly dropped when it emerged that the Foreign Office had previously admitted that the disclosures were not damaging at all and the case seemed to be more about governmental embarrassment than national security and public safety. Cathy Massiter, the MI5 officer who revealed details of its espionage operations against trade unionists and civil libertarians

and was motivated by her conscience, was ultimately not prosecuted under the 1911 Act but now she would have no defence at all under the 1989 Act.

Whilst opinions may differ on the strength of the public interest in each of these cases, the case for a jury making a decision on whether the disclosures were in the public interest could not be stronger. Surely a statutory public interest defence is preferable to prosecutors' unaccountable decisions behind closed doors or disobedient jurors ignoring the trial judge's directions or contrived defences which seek to import public interest via the backdoor.

The law is also deployed inconsistently with the result that it is rarely used against Government Ministers or MPs, for example, in circumstances when it would be against other citizens. When the Daily Telegraph published details of the Government's plans to kidnap Mahatma Gandhi and its editors revealed their source was the Home Secretary, unsurprisingly, he was not prosecuted. Yet David Shayler's revelation concerning the security services' alleged plot against Colonel Gaddafi was met with prosecution. When the Home Secretary made sensitive disclosures concerning the Westland affair these went unpunished as did Cecil Parkinson's alleged revelations of War Cabinet proceedings to his lover. Because Parliamentary privilege apparently protects any disclosures made by MPs, however damaging to national security, details of Kim Philby's treason and Colonel B's identity, for example, were disclosed by questions in the House and might well have been prosecuted if made outside it. Although the importance of Parliamentary privilege cannot be overstated, it ought not to be a public interest safety valve merely because there is no proper statutory defence in place.

Precedents for a public interest defence

There are plenty of precedents for the introduction of a public interest defence: in the context of Official Secrets, such defences exist in a number of different countries and a public interest defence has been read into the European Convention on Human Rights in the case law on Article 10. In domestic law, in other contexts relating to publication of material (either personal data or obscene publications, for example) analogous defences also exist. The introduction of a public interest defence as part of the Official Secrets regime would not, therefore, be radical: it would be a tried and tested means of attaining a defensible balance between the rights and interests at stake. As noted above, some form of public interest defence is in force in New Zealand, Australia and Canada, putting the UK (with the USA) in a minority among Five Eyes states. A summary of the national security law and associated public interest defences in these jurisdictions is attached as an appendix to this Paper.

Public interest defence in other countries

By section 15 of Canada's Security of Information Act 2001, it is a defence to an allegation of communicating or confirming special operational information, if the individual acted in the public interest. The public interest is assessed by reference to (i) the subject matter of the disclosed information (which must relate to a criminal offence being committed by a person in purported performance of public functions) and (ii) whether the public interest in disclosure outweighs the public interest in non-disclosure. The latter assessment must be conducted by reference to a defined list of additional considerations, including whether the extent of the disclosure is no more than reasonably necessary to disclose the alleged offence or prevent its commission or continuance, the seriousness of the alleged offence, whether the person took other reasonable steps before making the disclosure, whether they had reasonable grounds to believe the disclosure was in the public interest, and the extent of harm created by the disclosure. In this way, the manner and extent of the disclosure, and damage caused by it, can all be taken into account in determining whether the individual's conduct should attract criminal liability.

Denmark has a similar defence where the person making the disclosure is acting in "the legitimate exercise of obvious public interest". In Australia, too, it is a defence under Division 122.5(6) of the Criminal Code (as introduced by the National Security Legislation Amendment (Espionage and Foreign Interference Act) 2018) for a journalist to disclose protected information in the public interest.

The example provided by these jurisdictions shows that a public interest defence works, and that it does not lead to a flood of unauthorised damaging disclosures or an excessive risk to national security. Indeed, the Bar Council and Criminal Bar Association in their joint response to the Law Commission's consultation underscored that – while a public interest defence is a necessary part of a fit-for-purpose statutory framework, "The limited evidence from Canada and Denmark – jurisdictions which have enacted public interest defences in official secret cases – suggest that it will only be rarely, if at all, where the need will arise for reliance on the defence".

Precedents in UK law

Indeed, the UK courts and legislative framework generally have shown themselves able to handle public interest defences with relative ease. There is an existing "public good" defence to publication of obscene material, pursuant to section 4(1) of the Obscene Publications Act 1959, and a "public interest" defence to unlawfully obtaining personal data in section 170 of the Data Protection Act 2018. So, too, is there a public interest defence to the unauthorised disclosure of personal information in section 41(2)(k) of the Digital Economy Act 2017. In that provision, the public interest is defined as (i) preventing serious physical harm to a person, (ii) preventing loss of human life, (iii) safeguarding vulnerable adults and children, (iv) responding to an emergency, or (v) protecting national security.

Perhaps the most directly analogous example in UK law is provided by the Public Interest Disclosure Act 1998. That Act inserts into the Employment Rights Act 1996 a category of qualifying disclosures (in the employment context) that are identified as being inherently in the public interest. A disclosure is protected if the individual reasonably believed it was necessary to expose (i) commission of a criminal offence, (ii) a failure to comply with a legal obligation, (iii) a miscarriage of justice, (iv) danger to the health and safety of any individual (v) danger to the environment, and (vi) information tending to show that any of the above is being concealed. If a disclosure falls within those categories, the person making the disclosure is protected from adverse employment sanction. Factors which are taken into account in assessing the public interest include the seriousness of the relevant failure which is being revealed; whether it is continuing or is likely to occur in the future; the identity of the person to whom the disclosure is made and whether disclosure to 'the world at large' rather than a more limited class was reasonable.

These examples show that UK law is already adept at handling questions of public interest, including as a defence to otherwise criminal conduct. The creation of a public interest defence in the Official Secrets context would, therefore, be firmly based on well-established precedent.

Alex Bailin QC and Jessica Jones
matrix chambers
Mishcon de Reya LLP
November 2020

Appendix

Official Secrets Act - Public Interest Defence Project
A summary of approaches by "Five Eyes" jurisdictions to public interest disclosure

Australia

The National Security Legislation Amendment (Espionage and Foreign Interference) Act 2018 repealed sections 70 and 79 of the Crimes Act 1914, which criminalised the disclosure of confidential information without authorisation, and replaced it with Part 5.6 of the Criminal Code 1995. The Crimes Act 1914 did not allow for disclosure in the public interest, although it was a factor that could be taken into account on sentence[1].

Division 122.1 of the Criminal Code, as amended by the National Security Legislation Amendment (Espionage and Foreign Interference) Act 2018, makes it an offence for a person to communicate, deal with or remove from a proper place of custody "inherently harmful information", where that information was made or obtained by the person by reason of him or her being, or having been a Commonwealth officer or engaged by a Commonwealth entity. Inherently harmful information in the revised Code includes security classified information; information obtained by or made on behalf of a domestic or foreign intelligence agency; and information relating to the operations, capabilities or technologies of, or methods or sources used by, a domestic or foreign law enforcement agency.

Division 122.2 makes it an offence to communicate or deal with information in a way which causes or is likely to cause harm to Australia's interests, where that information was made or obtained by the person by reason of him or her being, or having been a Commonwealth officer or engaged by a Commonwealth entity. The term "communicate" in the Division includes publishing or making available. If the person by virtue of his office, is under a duty not to disclose information and he or she communicates it, then a further offence is committed: see Division 122.4.

Division 122.4A criminalises the communication of information by a non-government individual who has received information from a Commonwealth Officer or entity where that information is security classified as secret or top secret, damages security and or defence of Australia, interferes with or prejudices law enforcement, or harms or prejudices the health and safety of the public.

Defences are provided by Division 122.5 of the Criminal Code. Three defences are of interest: first, it is a defence to a prosecution for an offence under the Division that the person communicated the relevant information to the Inspector General of Intelligence and Security or other listed 'integrity agency' or communicated the relevant information for the primary purpose of reporting a criminal offence or maladministration regarding law enforcement, including Australian Federal Police, to an appropriate agency of the Commonwealth, State or Territory, or to a court[2].

Second, Division 122.5 makes the public interest defence under the Public Interest Disclosure Act 2013 ('PIDA') available to those accused of disclosing inherently harmful information contrary to Division 122.1 in certain tightly defined circumstances: see Division 2 (ss.25 ff) of PIDA. Broadly speaking, a public interest disclosure is defined as a disclosure of information, by a person who is or has been public official, that is

- a disclosure within the government, to an authorised internal recipient or a supervisor, concerning suspected or probable illegal conduct or other wrongdoing (referred to as "disclosable conduct");
- a disclosure to anybody, if an internal disclosure of the information has not been adequately dealt with, and if the wider disclosure satisfies public interest requirements;
- a disclosure to anybody if there is substantial and imminent danger to health or safety; or
- a disclosure to an Australian legal practitioner.

In other words, the protection is afforded first for internal reporting purposes, and then for external purposes, only if necessary. In the context of this discussion, it is important to note that the protection does not extend to intelligence agency information, which is very widely defined in section 41 of the Act, and includes information that has been received from or originated with an intelligence agency; information that might reveal sources, technologies or operations deployed or conducted by such agencies; and even extends to "sensitive law enforcement information".

1. Walworth v Merit Protection Commissioner and Another [2007] FMCA 24, [49]–[63].
2. Division 122.5 (3), (4A) and (5).

Third, Division 122.5(6) creates a separate defence for those engaged in the business of news reporting or presenting current affairs, if the information is obtained, disclosed or dealt with in the course of that business and that person reasonably believed they were acting in the public interest. Note that under Division 122.5(7), a person cannot have reasonably believed it would be in the public interest if engaging in that conduct would result in the publication of the identity of ASIO (Security Intelligence Organisation) staff; reveal information about the national witness protection program and its participants; or was for the purpose of assisting a foreign intelligence agency or foreign military organisation. The Public interest is not otherwise defined in the Division.

Canada

The Security of Information Act 1985 ("SIA") creates a number of offences relating to the misuse or disclosure of secret information. The first category of offences relate to Canada's defence, and include[3]:

- The unauthorised communication, use, retention or failure to take reasonable care of any secret code word, password, sketch, plan, model, article, note, or information relating to a prohibited place or anything in a prohibited place. A prohibited place is defined as a defence related premises or land, whether private or state owned. Communication includes making available.
- Communication of material described above relating to munitions of war, to any foreign power, or in any other way prejudicial to the safety or interests of the State.
- Receiving the material described above, knowing or having reasonable ground to believe that the material was communicated to him or her in contravention of the Act, unless he or she proves it was received contrary to his or her desire.

There is no public interest defence available to a person accused of the above defence related offences.

The second category of offences created by the SIA are directed towards those who work in security and intelligence, who are described by the SIA as "those that are permanently bound to secrecy[4]. Such persons include current and former members of (inter alia) the Canadian Security Intelligence Service, the Communications Security Establishment, and the National Security and Intelligence Review Agency. Sections 13 and 14 of the SIA prohibit the intentional and unauthorised disclosure by such persons of information that either would be (if it were true) or is special operational information[5].

Special operational information under the SIA includes the following: the identity of confidential sources; military plans; the means of obtaining covert intelligence; the object of a covert investigation; the means used to protect or exploit intelligence; and, intelligence or other information in relation to or received from a foreign intelligence agency or terrorist group.

If a person charged with an offence contrary to sections 13 or 14 of the SIA can establish that he or she acted in the public interest, they are not guilty of an offence. The public interest defence is limited to acts, the purpose of which is to disclose an offence that the person reasonably believes has, is or is about to be committed by another in their purported performance of a function on behalf of the Government of Canada[6]. The public interest in disclosure must outweigh the public interest in non-disclosure[7].

Section 15(4) of the SIA sets out the factors that must be considered by a judge or court when addressing where the balance of public interest lies:

- Whether disclosure is no more than is reasonably necessary to disclose the offence or prevent the commission of the offence;
- The seriousness of the alleged offence;
- The extent to which relevant guidelines, policies or laws were followed as alternatives;
- Whether the person had reasonable grounds to believe that disclosure would be in the public interest;
- The public interest was intended to be served by the disclosure;
- The extent of the harm/risk of harm created by the disclosure;
- The existence of exigent circumstances justifying the disclosure.

Note however, that before a judge or court can assess the balance of public interest in the disclosure in accordance with the above criteria, the person must have brought his or her concern and provided all relevant information to the following persons or entities before making the relevant communication:

- The deputy head of his or her department or if not reasonably practicable, the Deputy Attorney General of Canada.
- The National Security and Intelligence Review Agency if a response has not been received within a reasonable time from the deputy head of department or Deputy Attorney General.

It is only if the relevant communication is made after a failure of the National Security and Intelligence Review Agency to respond within a reasonable time that a wider, public communication can fall to be considered as a public interest disclosure under section 15 of the SIA.

3. Section 4(1) of the SIA.
4. Section 8(1) of the SIA.
5. Section 13 and 14 of the SIA.
6. Section 15(2)(a) of the SIA.
7. Section 15(2)(b) of the SIA.

New Zealand

Espionage, the wrongful communication of classified information by persons who have national security clearance or to whom classified information has been disclosed in confidence, and the wrongful communication of official information in the knowledge that that the communication is likely to prejudice the security or defence of New Zealand are all offences contrary to section 78 ff. of the Crimes Act 1961 (as amended). There is no public interest defence available to a person who is accused of committing one or more of the specified offences contrary to section 78.

More recently, the New Zealand Parliament passed the Protected Disclosures Act 2000 (PDA), which permits employees to make protected disclosures about wrongdoing within their organisation if[8]:

- The information concerns serious wrongdoing in or by the organisation;
- The employee believes on reasonable grounds that the information is true or likely to be true;
- The employee wishes to disclose the information so that the serious wrongdoing can be investigated; and
- The employee wishes the disclosure to be protected.

Serious wrongdoing is defined by the PDA as the unlawful or corrupt use of public funds, an act, omission or course of conduct that constitutes a serious risk to public health or maintenance of the rule law (including the right to a fair trial), a criminal offence, or conduct by a public official that is oppressive, discriminatory, grossly negligence or that constitutes gross mismanagement.

Note that the PDA does not permit public disclosure: instead, the employee, who can be a person employed in the public sector or a public official - including a person employed by an intelligence or security agency or other public sector agency that deals with classified information[9] - must follow the disclosure protocol prescribed by the PDA if the disclosure is to be protected under the Act, and the person making the disclosure is to be immune from prosecution[10].

That protocol, insofar as it relates to those employed in the security and intelligence field, is as follows:

- The employee must disclose the information in the manner provided by internal procedures established by the relevant agency. Those internal procedures must provide that the person to whom the disclosure is made has appropriate security clearance.
- A disclosure may be made by such a person to the head or deputy head of the relevant agency if it does not have internal procedures for receiving or dealing with information about serious wrongdoing, or the person making the disclosure reasonably believes the person to whom the wrongdoing should be reported is or may be involved in the serious wrongdoing alleged in the disclosure or is associated with someone who is or may be involved in the wrongdoing.
- A disclosure may be made by such a person to the Inspector General of Intelligence and Security, if the person making the disclosure reasonably believes that the head of the agency is or may be involved in the serious wrongdoing, or an immediate reference to the Inspector General is justified as a matter of urgency or for some other exceptional reason, or there has been no action following a disclosure of serious wrongdoing for 20 working days.
- A disclosure may be made to the Minster responsible for the relevant agency or the Prime Minister, if the disclosure has already been made as described above, and the person making the disclosure believes that the person to whom the disclosure was made has decided not to investigate the matter, or has not made progress with the investigation within a reasonable time, or has failed to take any action following an investigation, and the person making the disclosure continues to believe that the allegation of serious wrongdoing is true.

There is an additional wrinkle introduced by the Intelligence and Security Act 2017 to the protocol introduced by the PDA. Under section 160 of the 2017 Act, an employee of an intelligence and security agency must not suffer penalty or discriminatory treatment in relation to their employment by reason of having brought "a matter to the attention" of the Inspector General of Intelligence and Security unless the Inspector General determines that the employee did not act in good faith.

Finally, there appears to be some limited scope for the publication of protected disclosures about serious wrong doing in the event that the disclosure is made (by way of a complaint or otherwise) to the Inspector General of Intelligence and Security in the manner described above. Under section 6 subheading 1 of the Intelligence and Security Act 2017 the Inspector General can commence an investigation of his own motion in a wide range of circumstances, including "any matter relating to an intelligence and security agency's compliance with New Zealand law" or "into the propriety of particular activities of an intelligence and security agency"[11]. The Inspector General has wide-ranging investigative powers including the right to summons witnesses and require the disclosure of documents, and although the inquiry must be conducted in private, the Inspector General is required to produce a written report at its conclusion[12].

Such a report must be published on the Inspector General's website, although inevitably, any such reports are likely to be heavily circumscribed given the subject matter: for example, no information may be publicly disclosed in the report that "would be likely to prejudice the continued performance of the functions of an intelligence and security agency"[13].

8. Section 6 of the Protected Disclosures Act 2000.
9. Section 12 of the PDA.
10. Sections 7 to 18 of the PDA.
11. Section 18 Intelligence and Security Act 2017
12. Section 185 of the Intelligence and Security Act 2017
13. Section 188 of the Intelligence and Security Act 2017

The United States

18 USC, Chapter 37 (The Espionage Act 1917) of the US Code contains offences relating to espionage and censorship, including the offences of gathering, transmitting or losing defence information and unauthorised disclosure of classified information.

There is no public interest defence to unauthorised disclosures.

Section 798 of the Code makes it an offence to "knowingly and wilfully communicate, furnish, transmit, or otherwise make available to an unauthorized person, or publish, or use in any manner prejudicial to the safety or interest of the United States or for the benefit of any foreign government to the detriment of the United States any classified information".

Mishcon de Reya LLP
Africa House
70 Kingsway
London WC2B 6AH

T +44 20 3321 7000
F +44 20 7404 5982
E contactus@mishcon.com

mishcon.com

Mishcon de Reya