Whistleblowing in the Security Sector

Benjamin S. Buckland and Aidan Wills[1]

This chapter originally appeared in the following publication. This is an unedited English language version.

Title: *Protection of Whistleblowers*
Editors: Ms Nevena Ruzic and Ms Bojana Medenica
Publisher: Commissioner for Information of Public Importance and Personal Data Protection, Belgrade, 2013
Available (in Serbian only):
http://www.poverenik.rs/images/stories/dokumentacija-nova/Publikacije/Uzbunjivaci/zastita%20uzbunjivaca_kraj.pdf

Introduction

Public interest disclosures by (former) employees of security sector organisations are the most contentious area of whistleblowing. Intelligence and security services, police and armed forces have recourse to powers and resources that, if misused, can have serious implications human rights and public safety. Yet, of all employees, people who work in this sector have very few options for disclosing information showing wrongdoing and they are seldom well protected when they do so.

Whistleblowing by security sector personnel has rarely left the headlines in recent years. Revelations by Edward Snowden and many others have forced policymakers to consider how and what information should be kept secret and in which circumstances it can be made public. The decision of Snowden and others to go directly to the media with their information suggests that, at the very least, they had little faith in authorised channels for raising the alarm—little faith that such channels would be effective and little faith that they would be protected from retaliation by using them.

[1] bbuckland@mac.com and aidan.wills@gmail.com

In writing this chapter, we begin with a number of assumptions. Firstly, classification and confidentiality is essential—some information must be secret in order for government to function and to protect legitimate national security interests. Secondly, however, information that shows serious wrongdoing should not be kept secret; it must be made available to institutions of democratic oversight and, in some circumstances, the public at large. It is the goal of a whistleblower protection system—particularly one that covers the security sector—to find a middle ground between these two ideas.

Much of the debate on this issue has focused on irrelevant issues regarding the perceived heroism or treachery of various individuals. The aim of this chapter is, instead, to put forward proposals for a workable and balanced system for security sector whistleblowing. As such, the chapter can be read alongside the relevant section of the Global Principles on National Security and the Right to Information (the "Tshwane Principles"),[2] which set out how such a system could function in very precise terms. These principles have since been endorsed by the Parliamentary Assembly of the Council of Europe, which highlighted, in particular, the fact that "a person who discloses wrongdoings in the public interest (whistle-blower) should be protected from any type of retaliation, provided he or she acted in good faith and followed applicable procedures."[3]

The term 'whistleblower' is subject to a multitude of definitions and does not translate well into many languages. There are, however, a number of common elements which can be distilled from legislation and other sources. These elements make up the core of the whistleblowing definition used in this text.

> (1) Definitions commonly make reference to the types of conduct that may be disclosed; namely, real or perceived wrongdoing including (unlawful, irregular, immoral or illegitimate conduct) within a given organisation.[4]

---

[2] A copy of the principles is available at: http://www.opensocietyfoundations.org/publications/global-principles-national-security-and-freedom-information-tshwane-principles. The authors were heavily involved in drafting these principles.
[3] Parliamentary Assembly of the Council of Europe, Resolution 1954 (2013), para. 9.
[4] South Africa Protected Disclosures Act, 2000; John Bowers, Martin Fodder, Jeremy Lewis, Jack Mitchell, *Whistleblowing: Law and Practice* (Oxford: Oxford University Press, 2010), 1; Transparency International,

(2) Definitions frequently refer to the character of the wrongdoing being disclosed. Notably, definitions often make reference to the fact that wrongdoing (or potential wrongdoing) being disclosed must adversely affect (directly or indirectly) the public interest, as opposed to interests which are merely personal or private.[5] This aspect of the definition is reflected in the fact that a great deal of legislation on the issue includes the phrase public interest in the title.[6]

(3) Definitions generally refer to the fact that disclosures are made by members or former members (individuals or groups) of an organisation.[7]

This chapter focuses on the disclosure of information showing wrongdoing (hereafter *whistleblowing*) by employees, former employees, conscripts, and contractors of security sector organisations such as the police, military and intelligence services (hereafter, *security sector personnel*), as well as members of the executive branch working in national security related departments. It is divided into four main sections. The first looks at types of wrongdoing that may be disclosed, as well as at issues around classification, motive, proof and who may make a disclosure. The second part looks at internal and external channels for making disclosures, section three deals with reprisals and protections and the final section looks at disclosures to the media and public at large.

Recommended Draft Principles for Whistleblowing Legislation (Berlin: TI, November 2009), Principle 1; Roberts, Olsen and Brown, "Whistling while they work," 12; Japan "Public Interest Speak Up Advisors" in Richard Calland and Guy Dehn, eds., *Whistleblowing Around the World: Law, Culture and Practice* (Cape Town and London: ODAC/PCAW, 2004); M. P. Miceli and J. P. Near, "The Relationships Among Beliefs, Organisational Position and Whistle-blowing Status: A Discriminant Analysis" *Academy of Management Journal* 27, no. 4 (1984): 689.

[5] Roberts, Olsen and Brown, "Whistling while they work," 12; Peter Boden "Submission to the House of Representatives Standing Committee on Legal and Constitutional Affairs' Inquiry into Whistleblowing Protections within the Australian Government Public Sector," 29.

[6] See, for example, the Indian Public Interest Disclosure and Protection to Persons Making the Disclosure Bill 2010; New Zealand Protected Disclosures Act 2000; and the British Public Interest Disclosure Act 1998.

[7] South Africa Protected Disclosures Act, 2000; Bowers, Fodder, Lewis, Mitchell, *Whistleblowing: Law and Practice*, 1; Roberts, Olsen and Brown, "Whistling while they work," 12; M. P. Miceli and J. P. Near, "The Relationships Among Beliefs, Organisational Position and Whistle-blowing Status: A Discriminant Analysis" *Academy of Management Journal* 27, no. 4 (1984): 689.

Section 1: Types of wrongdoing, classification, motive, proof, who may make a disclosure.

1.1 Types of wrongdoing

The systems of protected disclosure which appear to best protect whistleblowers and encourage disclosures, are those that define as broadly as possible the types of wrongdoing that can be disclosed.[8] Legislation that encourages disclosures tends to be worded in a way that is unambiguous, so as not to leave a potential whistleblower guessing about whether the information they hold is covered by the law. This is particularly important in the security sector, where the classified or otherwise confidential nature of the material can make it difficult or, indeed, impossible for a potential whistleblower to obtain independent legal or other advice before making a disclosure.

As well as defining categories of information as broadly and unambiguously as possible, legislation designed to encourage disclosures also tends to clearly state that the seriousness or otherwise of an allegations should not affect whether or not a disclosure is protected.[9] Those tasked with receiving and investigating disclosures, rather than any individual employee of a security sector organisation, should make a determination as to whether it is worth investigating further.

Typical types of wrongdoing included in legislation include the following categories:[10]

1. criminal offences (some jurisdictions have chosen to define this broadly, while others have sought to carefully list every example that the law might cover).[11]

---

[8] Roberts, Olsen and Brown, "Whistling while they work," 45.

[9] Australian Federal Police. "Submission to the House of Representatives Standing Committee on Legal and Constitutional Affairs' Inquiry into Whistleblowing Protections within the Australian Government Public Sector."
http://www.aph.gov.au/Parliamentary_Business/Committees/House_of_Representatives_Committees?url=/laca/whistleblowing/subs.htm

[10] These provisions are drawn from, *inter alia,* Romania, Law on the Protection of Public Officials Complaining About Violations of the Law. Law 571/2004, Article 5; Canada, Public Servants Disclosure Protection Act, 2005, c.46, Article 8; United Kingdom, Public Interest Disclosure Act, 1998. Chapter 23, Section 43b; South Africa, Protected Disclosures Act, Act no.26 of 2000, Section 1(i). See for a detailed overview of different categories of wrongdoing, see also, Parliament of Australia, House of Representatives Standing Committee on Legal and Constitutional Affairs, *Whistleblower protection.*

2. dangers to public health and safety;
3. dangers to the environment;
4. abuse of public office;
5. miscarriages of justice;
6. significant mismanagement;
7. other matters in the public interest; and
8. deliberate concealment of any matter falling into to one of the above categories.

It is also important that the law captures the temporal element of wrongdoing. In the Republic of Korea, for instance, the law refers to crimes that have been committed, are being committed or are even likely to be committed.[12]

One final point can be made regarding categories of information. It is important that disclosure regimes provide automatic and unambiguous protection for anyone making a disclosure of information showing wrongdoing that falls into one of the categories defined by law. There is a clear danger, with regards to disclosures made by security sector personnel, that national security concerns are invoked to override the proper investigation of wrongdoing. If a disclosure regime clearly identifies categories of wrongdoing that are sufficiently serious (and establishes proper channels for disclosing such information), then a national security "imperative" should never form the basis of a justification for reprisal or prosecution, so long as the whistleblower makes use of such channels. In our view, information showing serious wrongdoing, such as torture (to take

[11] With regard to corruption, for example, this approach has been taken by the Australian (NSW) Independent Commission Against Corruption Act of 1988, which provides an extremely exhaustive list of relevant activities. The Independent Commission Against Corruption Act (Act 35 of 1988) defines corruption in Section 8(2) as: "any conduct of any person (whether or not a public official) that affects 'the honest or impartial exercise of official functions by any public official … or any public authority'. official misconduct (including breach of trust, fraud in office, nonfeasance, misfeasance, malfeasance, oppression, extortion or imposition); bribery; blackmail; obtaining or offering secret commissions; fraud; theft; perverting the course of justice; embezzlement; election bribery; election funding offences; election fraud; treating; tax evasion; revenue evasion; currency violations; illegal drug dealings; illegal gambling; obtaining financial benefit by vice engaged in by others; bankruptcy and company violations; harbouring criminals; forgery; treason or other offences against the Sovereign; homicide or violence; matters of the same or a similar nature to any listed above or any conspiracy or attempt in relation to any of the above."

[12] Republic of Korea, Act on the Protection of Public Interest Whistleblowers, Act no. 10472, March 29, 2011, Article 6. See also the United Kingdom, *Public Interest Disclosure Act,* 1998.

a perhaps obvious example) should be disclosed regardless of the damage or embarrassment such a disclosure may cause.[13]

1.2 Classification and confidentiality

In relation to disclosures in the security sector, there is a tendency to think immediately about classified information. While the cases that have attracted the most media attention concern these types of information, it is important to recognise that we are here concerned with much broader classes of information. Of interest, of course, is information which cannot be disclosed because it pertains, for example, to an ongoing criminal investigation. Beyond information that is classified or otherwise confidential, it should be noted that many types of information that security sector whistleblowers might be seeking to disclose are neither classified nor related to ongoing operations or investigations. A common assumption exists that when we talk about security sector whistleblowing, we are automatically talking about classified information of a highly sensitive nature. The reality can be (and perhaps mostly is) much more mundane. In this sense, protected disclosures of information in the security sector are much closer to those in other parts of government than might be assumed from a cursory look at what aspects of the issue are covered in the press.

1.3 Motive

A person's motive for disclosing information showing wrongdoing is sometimes viewed as a relevant factor in determining whether a disclosure should be protected. Whistleblowers may have any number of reasons for making a disclosure including, for instance, malice or financial gain. Ultimately, these motives are irrelevant as long as a disclosure brings to light information showing wrongdoing. By way of example, the fact that a police officer loathes her or his superior (and may very well wish to see her or him leave the force) should not mean that the officer's disclosure is less likely to qualify for protection when they disclose information showing wrongdoing.[14]

---

[13] In practice, of course, it is not always so simple and what constitutes wrongdoing can sometimes be heavily contested. If the intelligence services collect information in compliance with an interpretation of national law—as is the case with much of the information disclosed by Snowden—is it wrongdoing?

[14] United States Senate, *Report of the Committee on Homeland Security and Government Affairs, to accompany S. 743*. Report 112-155, 19 April 2012, 5.

Furthermore, the possibility that questions about motive may be raised in court may have a significant chilling effect on the willingness of persons to come forward with information showing wrongdoing. Public Concern at Work (a British whistleblower protection charity) argued for a number of years that the good faith requirement tempts lawyers to argue about motives in every case, something which resulted in amendments to the UK law in 2013.[15] This may also be the reason why such a test is not included in, for example, the public interest disclosure statutes of the Republic of Korea and New Zealand.[16]

1.4 Proof

With regards to the question of whether or not a whistleblower needs to provide proof to substantiate their disclosure, national law is fairly consistent. Most states opt for some variation on the "honest and reasonable belief" test. This standard requires that a person making a disclosure should have "an honest and reasonable belief" that his/her disclosure relates to a category of wrongdoing that is set out in the law.[17] Such a standard excludes from protection disclosures that are knowingly false[18] but still protects those that are not ultimately substantiated.[19]

A person making a disclosure should not be expected to prove that their information is accurate in order for their disclosure to be protected. What matters is that it was made in the reasonable belief that it was correct.[20] There are several key reasons for this. First, demanding proof from a person making a disclosure may encourage them to engage in illegal or contractually prohibited behaviour (such as accessing and retaining files that they are not authorised to have in their possession). Second, by gathering evidence, they may, in fact, taint it to the point that it is unusable by any official investigation. Third, attempts to gather proof may alert any wrongdoers that their activities have been

---

[15] *Enterprise and Regulatory Reform Act 2013*; see also: Public Concern at Work, "Good faith" - case law on PIDA.
[16] Republic of Korea, *Act on the Protection of Public Interest Whistleblowers,* Act no. 10472, March 29, 2011; New Zealand, *Protected Disclosures Act,* 2000.
[17] OECD, *Study on G20 Whistleblower Protection Frameworks: Compendium of Best Practices and Guiding Principles for Legislation* (Paris: OECD, 2012), 8.
[18] See, for example, Republic of Korea, *Act on the Protection of Public Interest Whistleblowers,* Act no. 10472, March 29, 2011, Article 2.2(a); see also, Parliament of Australia, Whistleblower protection, 85.
[19] Parliament of Australia, Whistleblower protection, 75.
[20] For supporting examples, see Kaplan, "The International Emergence of Legal Protections for Whistleblowers," 38; Transparency International, "Recommended Draft Principles for Whistleblowing Legislation," 2009, principle 6. Australian Law Reform Commission, *Secrecy Laws and Open Government in Australia*, 60.

discovered, thus leading to the destruction of evidence. It is much better, as one expert interviewed for this study quipped, that investigators find incriminating material in the company safe than an employee, seeking proof, breaks into it in the dead of night.[21]

1.5 Who may make a disclosure?

There is a great deal of variation in national law regarding who is eligible for protection from reprisals under protected disclosure regimes. In our view, legislation in this area should cover current and former employees, conscripts, contractors and sub-contractors of agencies involved in the provision of national security, as well as employees of relevant ministries or departments. They are not only those most likely to have access to classified or otherwise confidential information, but they are those most vulnerable to reprisals.

Whether or not anonymous disclosures are useful and/or should be permitted is a matter for debate. In jurisdictions where such disclosures are restricted, it is possible that doing so makes whistleblowers more accountable and, also, easier to protect. It seems more logical, however, to allow receiving agencies to assess the information they receive on its merits and choose to investigate anonymous disclosures when such an investigation seems likely to uncover wrongdoing. It is worth noting here that even where anonymous disclosures are permitted, there may be limits to how thoroughly such disclosures can be investigated. It is also worth underlining that it is usually difficult or impossible for whistleblowers to remain anonymous. Those who receive disclosures have a duty to keep them confidential but safeguarding someone's anonymity is unlikely to be possible in a large number of cases.

[21] Interview with Howard Whitton, April 2011.

Section 2: Channels for making a disclosure

2.1 Internal disclosures

It is good practice for organisations to set up their own internal procedures for reporting and investigating allegations of wrongdoing, alongside statutory laws.[22] In some states, such as Norway and Romania, the law even obliges organisations to do this.[23] Internal bodies to which disclosures can be made might include: supervisors, employee representatives, human resources officers, lawyers, or even a dedicated internal complaints unit.

Internal procedures have two functions. Firstly, they provide a channel through which disclosures can be made and hopefully acted upon. If effective, internal channels can be the simplest and most effective means of addressing wrongdoing. Indeed, it is often regarded as preferable to resolve problems at the lowest level possible. When classified or otherwise confidential information is involved, good internal procedures can ensure that information never leaves the ring of secrecy, while still providing an opportunity for security sector personnel to report wrongdoing (although this can also be achieved if disclosures are made to designated independent bodies; see the following section for details). Secondly, strong internal procedures are an important way for an organisation to demonstrate a commitment to whistleblowing in general, even if employees ultimately choose to make disclosures to independent bodies instead.[24]

In an ideal situation, concerns raised about wrongdoing would be dealt with efficiently and effectively by a line manager within the organisation concerned.[25] As the Australian Commonwealth Ombudsman has argued, this should remain the preference, both legislatively and practically.[26] However, while the existence of internal procedures is

---

[22] Parliamentary Assembly of the Council of Europe, Committee on Legal Affairs and Human Rights. "The protection of whistle-blowers," 21.
[23] Romania, *Law on the Protection of Public Officials Complaining About Violations of the Law 2004*; Norway, *Working Environment Act 2005* and ethical guidelines for the public service.
[24] Roberts, Olsen and Brown, "Whistling while they work," 23-24.
[25] Roberts, Olsen and Brown, "Whistling while they work," 48.
[26] see Australian Law Reform Commission. *Keeping Secrets: The Protection of Classified Information and Security Sensitive Information*, Report 98 (Canberra, May 2004), 81.

essential for the reasons outlined above, they are also problematic, particularly where people within the chain of command are complicit in wrongdoing.

2.2 Disclosures to independent oversight bodies

For the purposes of this chapter, "independent oversight bodies" are defined as entities that are both institutionally and operationally independent from the agency and/or department that the person works for. They are bodies that are not only external to the security sector organisation concerned but are also outside the executive branch ministry or department that has political responsibility for a particular organisation. In most jurisdictions, these are probably the weakest link in the chain for security sector whistleblowers. It is likely, for example, that Snowden went directly to the media in part because external channels either did not exist or were grossly inadequate.

The independent oversight bodies to which whistleblowers may make disclosures fall into three broad categories:

1. institutions that are established for the specific purpose of receiving and investigating disclosures from whistleblowers (e.g., the Canadian Public Sector Integrity Commissioner and the US Office of Special Counsel);
2. institutions with a mandate to oversee the agency or sector concerned (for example, some inspectors general, and parliamentary committees); and
3. bodies which have a mandate to oversee and receive complaints from all areas of the public (and sometimes private) sector (for example, general ombuds institutions and anti-corruption commissions).

The independent oversight bodies that are authorised to receive and investigate disclosures from members of security sector organisations are normally different from those authorised to receive disclosures from public sector organisations more generally. These bodies are typically authorised to handle classified information and usually have a legal mandate to oversee the work of particular security sector organisations. This distinction can largely be explained by the understandable desire of governments to protect information. For example, under the New Zealand Protected Disclosures Act, employees of an intelligence or security agency may only make disclosures to the

Inspector General of Intelligence and Security,[27] an oversight body which is officially independent from the intelligence and security agencies and the executive.[28]

Theoretically, independent oversight bodies can play three principal roles regarding whistleblowers:

1. they are authorised to receive and investigate information showing wrongdoing from whistleblowers;
2. they formulate recommendations and may even be empowered to issue orders to address wrongdoing raised by whistleblowers;
3. they may address claims of retaliation against whistleblowers taken as a result of their disclosures.

In the security sector, most independent oversight bodies focus on the first of these three roles.

2.2.1. The importance of external channels for making disclosures

The desire of governments and their agencies to protect information pertaining to the work of security sector organisations has, unfortunately, led to significant limitations (and in some cases outright prohibitions) on disclosures to external bodies by employees of such agencies. This is problematic because, in the security sector, it is particularly important for personnel to have the option of disclosing information showing wrongdoing to an independent oversight body authorised to receive and investigate this information, even when such information is classified or otherwise confidential. This is for a number of reasons.

Firstly, in any system for the reception and investigation of complaints or concerns it is not optimal for complaints to be investigated by the same body implicated in these complaints. There is an inevitable risk that there will be a conflict of interest if disclosures of information showing wrongdoing within an organisation are handled exclusively within the organisation. Desires to protect reputations, friendships and career prospects are likely to conflict with the need for allegations of wrongdoing to be fully investigated and addressed. Additionally, disclosures made internally may be more

[27] New Zealand, *Protected Disclosures Act,* 2000, S.12.
[28] It should be noted that the independence of this body has been challenged, see for example, *Zaoui v. Greig,* High Court of New Zealand, CIV-2004-404-317, 31 March 2004.

likely to result in the destruction of evidence or other practices which would compromise the proper investigation and rectification of wrongdoing.

Secondly, research has demonstrated that in many contexts would-be whistleblowers lack faith in the capacity of internal mechanisms to both fully investigate allegations of wrongdoing and to protect them from reprisals in doing so.[29] This is closely related to the fact that, as we have already noted, organisational cultures within security sector organisations tend to deride whistleblowing. As a result, disclosures made internally are highly likely to result in retaliatory action against the whistleblower.

Thirdly, the discretionary nature of the powers available to security sector organisations and the potential that the misuse of such powers can result corruption or in serious human rights violations, makes it all the more important that wrongdoing can be disclosed to an independent body.

Finally, the availability of effective independent bodies for the receipt and investigation of information showing wrongdoing may make it less likely that whistleblowers will turn to the media. This is ultimately, in the interests of the whistleblower (who is unlikely to face prosecution for the unauthorised disclosure of information), security sector organisations and the public at large (both of whom have an interest in the protection of information that is properly classified).

While independent oversight bodies provide an essential outlet for security sector personnel to raise concerns, whistleblowers can also contribute to the work of these oversight bodies by providing them with information. Indeed, whistleblowers can play a key role in alerting overseers to potential problems which need to be examined and/or may form part of broader investigations they are undertaking. Although some oversight bodies have the authority to question any employee of a given agency, most of their information comes from senior management and the executive branch. If a system of disclosures to independent oversight bodies works properly, whistleblowers can function as an 'early warning system' for overseers by providing them with information

[29] Roberts, Olsen and Brown, "Whistling while they work," 5.

about serious problems which may not be readily reported to them by agency directors or the executive branch.

2.2.2. Disclosures to parliament

In some states whistleblowers are authorised by law to disclose information showing wrongdoing to members of committees of parliament, although, in view of recent events in the US, it is important to emphasise the fact that the effectiveness of disclosures to independent bodies made up of politicians are contingent upon those politicians believing that it is in their political interests to tackle an issue. Recent US history has shown that national security oversight is a hot potato and no politicians want to be seen as weak on the issue. Whistleblowers should not have to rely for protection on the political winds of the day.

Where such procedures do exist, disclosures have, most commonly, to be made to designated parliamentary oversight committees in order for them to be protected. Such committees are typically those responsible for security matters, for example, intelligence oversight committees, armed forces committees and internal security committees. These committees usually operate within the ring of secrecy, meaning that they are ordinarily able to view classified information. Accordingly, such committees hold some or all meetings *in camera,* have appropriate physical measures in place to protect information, have a security cleared staff to receive disclosures and, depending on the system, may also have security cleared members.

Elsewhere, disclosures made to parliament are characterised as being equivalent to disclosures to the public. This is most likely the case in states where no parliamentarians are permitted to access classified information, as is the situation, for example, in Ireland.

Whether or not whistleblowers are legally permitted to disclosure information to parliament depends largely on the question of whether a particular member of parliament or parliamentary entity is competent to view classified information. Such competence is typically conferred by virtue of a parliamentarian's membership of a certain committee (for example, the Italian Parliament's Committee for the Security of

the Republic) or by their status a party leader and/or a speaker of parliament.[30] Whether or not an MP has security clearance is of limited relevance to this question. A minority of states require that members of certain committees are vetted and given clearance in order to access classified information (this is the case, for example, in many post-communist states in Eastern Europe). In the majority of states in the EU, as well as the US, however, parliamentarians do not require a security clearance to access classified information as part of their work. In these cases, parliamentarians are deemed competent to view such information by virtue of their position as democratically elected representatives.[31]

A further consideration, which may be considered relevant in some contexts, is the question of whether given parliamentarians may have a "need to know" particular information. We argue that, at the very least, membership of a committee with responsibility for security or security sector organisations confers a manifest "need to know" information originating from these entities. Hence, members have a clear "need to know" with regards to information that might be disclosed to them by a whistleblower. More generally, it can be contended that all parliamentarians have a need/right to know information about wrongdoing within the executive branch and its agencies (across all policy areas) by simple virtue of their status as democratically elected representatives.[32] While we do not agree entirely with this second viewpoint, we feel that parliament plays a crucial role in any comprehensive whistleblower protection regime and that whistleblowers should always be authorised to make disclosures of classified or otherwise confidential information to at least some subset of a parliament's members.

While parliamentary committees can provide a valuable channel for the disclosure of information showing wrongdoing, their effectiveness is often limited by a number of factors. Parliamentary committees are invariably dominated by the governing parties. As a consequence, they may not be well-suited to the impartial examination of certain types of information provided by whistleblowers. Indeed, members of parliamentary

[30] Aidan Wills and Mathias Vermeulen, *Parliamentary Oversight of Security and Intelligence Agencies in the European Union*, (Brussels: European Parliament 2011), Section 4.5.
[31] Wills and Buckland, *Access to Information.*
[32] Khemani, *The Protection of National Security Whistleblowers,* 13.

committees may have clear political incentives for not wishing to investigate or expose issues which may be acutely embarrassing for their colleagues in government or opposition, as well as detrimental to their own political futures. Furthermore, parliamentarians are not commonly specialists in security-related issues and, in many states, are not supported by adequate specialist staff. As a result, parliamentary committees may not have the requisite knowledge or expertise to conduct investigations relating to information showing wrongdoing in the security sector. The latter problem is compounded by the fact that parliamentarians are often overburdened and may be unable to devote the time or resources required to adequately exercise their oversight functions.[33]

Parliaments can, nevertheless, play a useful role in the investigation of information showing wrongdoing. Partisanship can (even when used for political point-scoring) help to ensure that even embarrassing information is exposed. Furthermore, due to their legislative and budgetary powers, parliaments may be well-positioned to promote compliance with their wishes regarding the righting of wrongs, as well as the protection of whistleblowers.

2.2.3. Disclosures to specialised non-parliamentary oversight bodies

Beyond parliamentary committees, some states have established specialised independent bodies to oversee various aspects of the work of security sector organisations. These non-parliamentary oversight bodies are generally led by one or a small group of senior public figures (e.g. former judges, former prosecutors, and former politicians) supported by a professional staff. Such bodies have become increasingly common in the oversight of security and intelligence and police services. Notable examples include: the Canadian Security Intelligence Review Committee (SIRC), and the Dutch Review Committee on the Intelligence and Security Services (CTIVD), and the Belgian Permanent Oversight Committee on the Police Services.

These specialised oversight bodies are normally authorised to receive disclosures from personnel of the agencies which they oversee and to investigate them accordingly. There

[33] Wills and Vermeulen, *Parliamentary Oversight of Security and Intelligence Agencies in the European Union.*

are significant advantages associated with making disclosures to specialised independent oversight bodies from the perspective of both the executive and, more importantly, the whistleblower.

Firstly, specialised independent oversight bodies are well-placed to examine disclosures of information showing wrongdoing because they have a mandate to oversee a particular service or sector on an ongoing basis. These mandates give them an understanding of the broader context and issues associated with a given agency or sector and this awareness may help them to spot linkages between information disclosed by a whistleblower and findings derived from their general oversight functions.

Specialised independent oversight bodies may also be better placed than their parliamentary counterparts to investigate disclosures of information showing wrongdoing because they are usually composed of subject matter experts. This is reinforced by the fact that they operate on a full-time basis and are typically better resourced than parliamentary committees with similar mandates.

Secondly, whistleblowers may be more likely to disclose information to an oversight body which is known and (hopefully) trusted to members of their organisation. In well-established oversight systems, security sector personnel should know that such bodies are authorised (and competent) to handle sensitive information. Nevertheless, a careful balance must be struck between the potential advantages of familiarity and the need for independence. Familiarity may be a disadvantage if the oversight body is too close to the senior leadership of the organisation.

Finally, specialised independent oversight bodies may be better placed to protect classified or confidential information than both their parliamentary counterparts and institutions that handle disclosures from the public sector more generally. While they are institutionally and operationally independent, such bodies may nevertheless operate within the ring of secrecy. In other words, they are authorised to receive and handle the highest level of classified or otherwise confidential information and have procedures in place to do so. From the point of view of security sector organisations and personnel,

this capacity to handle classified information (in combination with their small size) may make them preferable to other bodies as a channel for making external disclosures. Bodies that do not have a mandate to oversee the security sector may not have procedures in place to properly handle information of this type or may simply be unsure of to how to proceed when presented with such information.

2.2.4. Accessing independent oversight bodies

A first requirement for access to independent bodies by whistleblowers is that such channels must be "visible." Visibility is essential to ensure that wrongdoing is disclosed, but it may also reduce the likelihood of disclosures being made to an independent body that is not authorised to receive it (in some contexts a whistleblower could be prosecuted for making disclosures to such bodies).

Assuming that an independent oversight body is "visible" to potential whistleblowers, a second important consideration relating to access is whether or not members of security sector organisations have to exhaust, or at the very least, make use of internal disclosure mechanisms before approaching independent bodies.

Several overseers at a recent DCAF-OSF workshop argued that it is essential that security sector personnel have direct, unfettered access to independent bodies, should they wish to raise complaints or report concerns showing wrongdoing.[34] Indeed, it is noteworthy that legislation that applies to disclosures made outside the context of the security sector does not impose a requirement for a disclosure to first be made internally, particularly where such a disclosure pertains to a highly time sensitive issue, where a disclosure made through internal channels is likely to result in the destruction on concealment of evidence, or where an internal disclosure would be likely to result in reprisals against the individual making the disclosure.[35] In view of this and for the reasons outlined above (relating to the important of external channels for making protected disclosures), we are of the opinion that such persons should not have to first

[34] DCAF-OSF workshop held in Geneva, 4-5 May 2011.
[35] United Kingdom, *Public Interest Disclosure Act 1998*, Chapter 23, Section 43g; South Africa, *Protected Disclosures Act 2000*., Section 9; Canada, *Public Servants Disclosure Protection Act,* 2005, c.46, Section 16. This approach is also endorsed by the Parliamentary Assembly of the Council of Europe, Resolution 1729 on the 'Protection of "whistle-blowers,"' 29 April 2010, paragraph, 6.2.3.

make a disclosure to a superior, e.g., through the chain of command in the armed forces, or to an internal (or "quasi-internal") body.

A final point relating to accessing independent bodies relates to what such bodies must do with information they have received. It is clearly not sufficient for the law to simply designate or establish independent oversight bodies to which whistleblowers can make protected disclosures. These bodies also need clear guidance on what they are required to do with information received from whistleblowers. An examination of national laws and practice reveals that often, the law and subsidiary regulations give little guidance on these issues. In the Canadian case, for example, the law and subsidiary regulations do not state what either the Security Intelligence Review Committee (SIRC) or the Communications Security Establishment (CSE) Commissioner are meant to do with information pertaining to serious wrongdoing that they receive from whistleblowers.[36]

A related point is the question of whether an obligation should exist to take action on the part of independent oversight bodies. At a minimum, we would argue that overseers have a duty to properly assess all disclosures they receive, to determine whether they require further investigation by themselves or another competent body.[37]

Section3: Reprisals and protections.

3.1 Reprisals

Whistleblower protection legislation is premised on the recognition of two realities. First, some employers will retaliate against employees (and persons linked to them) for disclosing information showing wrongdoing within their organisation. Second, most employees with such information showing wrongdoing will not bring it to light unless they feel that they will be protected against possible reprisals for making a disclosure. Accordingly, whistleblower protection legislation aims to deter employers from retaliating against whistleblowers, and to provide recourse when reprisals do occur.

---

[36] Under section 15 of the Canadian *Security of Information Act*, government employees with privileged access to information, can disclose information showing serious wrongdoing to these bodies.
[37] Buckland and McDermott, *Ombuds Institutions for the Armed Forces,* Chapter 6.

Unfortunately, the situation regarding reprisals against whistleblowers – particularly those from within the security sector – is not pretty. This is the case in three main respects. First, protections offered by the law may be comprehensive but not adequately implemented. Second, legal protections may not go far enough to protect against common types of reprisal. Finally, the law in some states may offer no protection at all.

The lack of protection afforded to whistleblowers is particularly problematic because it can have a chilling effect on the likelihood that whistleblowers will come forward. This is supported by evidence such as one study of whistleblowers which found that 70 per cent of US federal employees claiming knowledge of corruption chose not to report it due to fear of reprisal.[38]

National laws use a litany of terms to refer to reprisals; these range from "occupational detriment,"[39] "disadvantageous measures,"[40] and "personnel actions."[41] Notwithstanding these semantic differences, all of these terms refer to negative actions taken in retaliation for the disclosure of information showing wrongdoing. Before turning to the types of action that may constitute a reprisal, it is important to make it clear that we are talking about reprisals resulting from disclosures made both externally and internally.[42] A comprehensive list of forms of reprisal (which should be prohibited) can be found in the Korean Act on the Protection of Public Interest Whistleblowers. The South African Protected Disclosures Act is similarly comprehensive and makes reference to the following forms of reprisal:

a) being subjected to any disciplinary action;
b) being dismissed, suspended, demoted, harassed or intimidated;
c) being transferred against his or her will;
d) being refused transfer or promotion;
e) being subjected to a term or condition of employment or retirement which is altered or kept altered to his or her disadvantage;

---

[38] Khemani, *The Protection of National Security Whistleblowers.*
[39] South Africa, *Protected Disclosures Act 2000*, Section 1(v).
[40] Republic of Korea, *Act on the Protection of Public Interest Whistleblowers 2011*.
[41] United States, 5 USC § 2302.
[42] Parliamentary Assembly of the Council of Europe, Committee on Legal Affairs and Human Rights. "The protection of whistle-blowers," 9.

f) being refused a reference or being provided with an adverse reference, from his or her employer;
g) being denied appointment to any employment, profession or office;
h) being threatened with any of the actions referred to paragraphs (a) to (g) above; or
i) being otherwise adversely affected in respect of his or her employment, profession or office, including employment opportunities and work security;[43]

To this list we can add the following forms of reprisal, based on research on security sector whistleblowers:

- conducting retaliatory investigations in order to divert attention from the issues that the whistleblower is trying to expose;
- ordering psychiatric tests or examinations;[44]
- conducting unlawful surveillance (particularly of an employee's communications with an independent oversight body);[45]
- physical and emotional abuse and intimidation; and
- security clearance suspension or revocation.[46]

Given their widespread use of revocation and suspension of security clearances in retaliation against security sector whistleblowers, it is worth examining these in more detail. In many cases, suspension or revocation of a security clearance may be tantamount to firing as, without their clearance, many security sector personnel are simply unable to perform their jobs.[47] The Korean Act on the Protection of Public Interest Whistleblowers addressees this issue by stating that "the suspension of access to security information or classified information; the cancellation of authorization to handle security information or classified information"[48] shall be punished "by imprisonment for not more than two years or by a fine not exceeding 20 million won."[49]

[43] See also the United States, 5 USC § 2302.
[44] United States, 5 USC § 2302.
[45] United States Office of Special Counsel, "Memorandum for Executive Departments and Agencies," 20 June 2012.
[46] See Republic of Korea, *Act on the Protection of Public Interest Whistleblowers 2011*, Article 6(e).
[47] United States Senate, *Report of the Committee on Homeland Security and Government Affairs,* 35.
[48] Republic of Korea, *Act on the Protection of Public Interest Whistleblowers 2011*, Article 6(e).
[49] Republic of Korea, *Act on the Protection of Public Interest Whistleblowers 2011*, Article 30(2)1.

3.2 Protections

Closely related to the preceding section on reprisals is the question of how whistleblowers can be protected from such actions.

3.2.1 Legal protections against reprisals

Protections against the types of reprisal outlined in the previous section are typically provided for by law but their scope differs significantly across jurisdictions. The exact phrasing of such legal protections varies across jurisdictions, with some laws placing the obligation on persons not to retaliate against whistleblowers and others framing it as a negative right, i.e. the right not to be retaliated against. Canadian law, for example, states that "no person shall take any reprisal against a public servant or direct that one be taken against a public servant."[50] British law, on the other hand, stipulates that "[a] worker has the right not to be subjected to any detriment by any act, or any deliberate failure to act, by his employer done on the ground that the worker has made a protected disclosure."[51]

Protection may be even stronger if the law explicitly provides whistleblowers with immunity from civil and criminal liability, as well as disciplinary proceedings arising from the disclosure of information showing wrongdoing in accordance with proscribed procedures.[52] The New Zealand Protected Disclosures Act is an example of a piece of legislation which provides such protection. It states that those making disclosures should not be "liable to any civil or criminal proceeding or to a disciplinary proceeding by reason of having made or referred that disclosure of information" and that such protections should apply "despite any prohibition of or restriction on the disclosure of information under any enactment, rule of law, contract, oath, or practice."[53] Employees of the New Zealand intelligence and security services are only permitted to make external disclosures to the Inspector General for Intelligence and Security. In doing so, they are protected against "any penalty or discriminatory treatment of any kind in relation to his or her employment" unless the IG determines that they did not act in good

[50] Canada, *Public Servants Disclosure Protection Act*, S.C. 2005, c. 46.
[51] United Kingdom, *Public Interest Disclosure Act 1998*.
[52] Transparency International, *Recommended Draft Principles,* principle 15.
[53] *Protected Disclosures Act 2000*.

faith. [54] Thus, protections apply to those who disclose information through proscribed channels regardless of its level of sensitivity or classification.

Needless to say, in New Zealand and elsewhere, legal provisions granting immunity from prosecution need to be read alongside other legal provisions that strictly limit the channels through which protected disclosures can be made by members of security sector organisations. Immunity would not ordinarily extend to disclosures which entail the commission of a criminal offence pertaining to the unauthorised release of classified or otherwise confidential information.

Disclosures made through the "wrong channels" are often not protected. This problem can arise when the law establishes or designates specific independent bodies to receive disclosures from whistleblowers but does not protect disclosures made to other independent bodies. In our view, this is problematic because making disclosures to the "correct" independent body is predicated on the whistleblower having a good understanding of the system. Such an understanding cannot be taken for granted, especially as it is often very difficult for those considering making a disclosure to seek advice internally or on where and how to make disclosures outside their organisation. For this reason, whistleblowers should ordinarily be protected if they unwittingly make a disclosure to the incorrect independent body. In such cases, it ought to be incumbent upon the recipient body to either transmit the disclosure to the appropriate body or advise the whistleblower of where and how they should make the disclosure.[55]

3.2.2 Confidentiality

Confidentiality relating to disclosures is another element of protection for whistleblowers. In general, this means that bodies tasked with receiving and investigating protected disclosures must not release information that might identify a whistleblower. The logic behind such requirements is that organisations cannot retaliate against employees for making disclosures if they cannot identify the person who made a disclosure.

---

[54] New Zealand, *Inspector-General of Intelligence and Security Act 1996,* Section 12.
[55] The latter requirement is included in the South Africa, *Protected Disclosures Act 2000*, Section 8(2).

There are exceptions to the general rule of confidentiality regarding disclosures. Most obviously, the whistleblower may give his/her consent (in writing) to his/her identity being revealed. The law may also authorise the body receiving a protected disclosure to identify a whistleblower if, for example, this is deemed to be necessary for the "effective investigation of the allegations," "to prevent serious risk to public health or public safety or the environment" or with "regard to the principles of natural justice."[56]

It is worth noting that, in the security sector, provisions on confidentiality may be largely symbolic. A minimum amount of information will often need to be shared with relevant parties as part of an investigation into a disclosure (made either internally or externally). In many cases, this will provide sufficient information for someone (e.g., a senior manager) with inside knowledge of an organisation's work to identify who made the disclosure. This is in large part due to the strict compartmentalisation of information within many security sector organisations, which means that very few people have access to information about specific programmes or activities. Moreover, in many states, security and intelligence services have relatively few personnel. This, of course, makes it easier for management to ascertain who made a disclosure. Also relevant is the fact that many security sector organisations specialise in information protection and investigation and they therefore have skills that facilitate the identification of whistleblower. In view of these considerations, we must remain cautious about the practical effect of legal guarantees of confidentiality for whistleblowers.

3.2.3 Penalties for retaliation against whistleblowers

In many jurisdictions, the law does not make clear exactly what penalties (if any) apply to those who retaliate against whistleblowers. Whether those who retaliate face consequences relies, in many jurisdictions, on the willingness or ability of the whistleblower to take action in court or to refer the issue to another independent body. In some jurisdictions, however, retaliation against whistleblowers is penalised or even criminalised.[57] This is the case, for example, in Hungary where the law states that "[a]ny person who takes any detrimental action against a person who has made an

[56] New Zealand, *Protected Disclosures Act 2000*, Section 19.
[57] Parliamentary Assembly of the Council of Europe, Committee on Legal Affairs and Human Rights. "The protection of whistle-blowers."

announcement of public concern is guilty of a misdemeanor and may be punished by imprisonment not to exceed two years, work in community service or a fine."[58] Similarly, in the Republic of Korea, the law states that retaliation against whistleblowers shall be punished "by imprisonment for not more than two years or by a fine not exceeding 20 million won."[59] Some prominent organisations, including Transparency International (in its Recommended Draft Principles for Whistleblower Legislation), have advocated such a practice. It remains controversial, however, with many suggesting that such penalties may be disproportionate.[60]

3.2.4 Capacity of internal and independent bodies to provide protection

Even where protections are provided for by law, a lack of capacity or of robust legal powers may still hamper internal or independent bodies' efforts to enforce them. It is particularly important that bodies to which protected disclosures can be made have real powers to protect whistleblowers from retaliation and the capacity to investigate and act against those who carry out such retaliation. The Australian Commonwealth Ombudsman and the Australian IGIS are examples of bodies that are authorised to receive disclosures of information showing wrongdoing but are said to lack the proper powers to prevent reprisals.[61] This weakness is shared by bodies in a number of other jurisdictions, including Germany and Belgium. For example, the Belgian Standing Intelligence Agencies Review Committee cannot take any direct action relating to retaliation against whistleblowers. It can only report matters to the judiciary or the relevant minister when cases of retaliation come to its attention.

3.2.5 Burden of proof regarding retaliation

Finally, there is some debate concerning where the burden of proof should lie regarding claims of retaliation against those who have made disclosures of information showing wrongdoing. It would be venturing too far to suggest that any disclosure of information showing wrongdoing should somehow immunise a whistleblower from all forms of adverse employment-related action for the rest of their career. Yet, at the same time, the

---

[58] Hungary, *Act IV of 1978 on the Criminal Code*, Section 257.
[59] Republic of Korea, *Act on the Protection of Public Interest Whistleblowers 2011*, Article 30(2)1.
[60] Transparency International, "Recommended Draft Principles for Whistleblowing Legislation," 2009, Principle 3.
[61] Australian Law Reform Commission, *Keeping Secrets,* 82.

burden of responsibility must lie with the employer to show that any adverse employment-related action is not precipitated by the fact that the person concerned has made a protected disclosure. This is the standard adopted by the Parliamentary Assembly of the Council of Europe, which has argued that "[i]t shall be up to the employer to establish beyond reasonable doubt that any measures taken to the detriment of the whistleblower were motivated by reasons other than the action of the whistleblower."[62] Given the information and power asymmetries inherent in any employee-employer relationship, it is clearly problematic to expect employees to go further than the Council of Europe standard and demonstrate that reprisals have occurred or are occurring as a result of their actions in making a disclosure.

Section 4: Disclosures to the media and public at large.

In addition to disclosures made through internal channels and to designated independent bodies (as discussed above), security sector personnel may choose to disclose information showing wrongdoing to the media and public at large. While doing so may be in violation of the law, historically, disclosures to the media have been instrumental in bringing to light a number of the most serious examples of wrongdoing in the security sector. Even setting aside the more recent revelations by Edward Snowden, it is not hard to make a long list of notable cases, including: the Iran Contra affair, Watergate, rendition and secret detention of suspected terrorists after 9/11, warrantless wiretapping, trafficking by international police contractors in Bosnia and Herzegovina, and the illegal surveillance of UN officials by a member state. Disclosures to the media and public at large are an essential alternative to disclosures to prescribed internal and independent bodies (discussed above) and should be regulated as part of a comprehensive approach to whistleblowing. The media relies on such disclosures to perform its function of holding government to account.

4.1 The media as a (more effective) last resort?

This section will show that disclosures are most commonly made to the media when persons with information showing wrongdoing made disclosures internally or to

[62] Parliamentary Assembly of the Council of Europe, Committee on Legal Affairs and Human Rights. "The protection of whistle-blowers," 3.

designated independent bodies, and not received a satisfactory response. Such persons may also approach the media directly because they believe that making disclosures to designated internal and/or external bodies would either lead to reprisals or would be ineffective.

Disclosures to the media and public at large can be viewed as an essential 'safety valve' when established procedures for receiving and investigating information showing wrongdoing are either inexistent or ineffective. They may also be considered when other options for bringing concerns to light have failed or would be futile.

Some commentators have asserted that the media is more effective at ensuring that concerns raised by whistleblowers receive due attention and are addressed in an appropriate manner.[63] The disclosure of information to the media may also expedite responses to allegations of serious wrongdoing, where persons have made disclosures through prescribed (internal or external) channels and the issues raised have not been investigated or addressed in a timely manner.[64] According to Ryan Check and Afsheen Radshan, "CIA whistleblowers may feel that taking their issues to the press is not only faster, but serves as greater punishment of the alleged violators."[65] Media organisations may also be more effective at exposing misconduct as well as at ensuring that the identities of persons making disclosures are concealed in order to reduce the risk of retaliation.[66]

4.2 Disclosures to the media outside the security sector

It is instructive to look at legislation on protected disclosures outside the specific context of the security sector which ordinarily protects disclosures of information to the media and the public at large. In our view, such legislation provides good practices which could potentially be extended to the security sector. In general, such legislation is based on considerations of the public interest.

---

[63] See, for example, Stephen Vladeck, "Left out in the cold: the chilling of speech, association, and the press in post-9/11 America," *American University Law Review*, 57 (June 2008).
[64] Parliament of Australia, House of Representatives Standing Committee on Legal and Constitutional Affairs, *Whistleblower protection,* 163.
[65] Check and Radsan, "One Lantern in the Darkest Night," 288.
[66] Cited in Khemani, *The Protection of National Security Whistleblowers,* 164.

Such legislation typically requires two sets of criteria to be met in order for a disclosure made to the media or public at large to be protected. The first set of criteria relates to the substance of the disclosure. The information must show wrongdoing of a particularly serious nature such as a serious violation of the law and/or an imminent risk of substantial danger to a person's life, health or safety, or the environment.

The second set of criteria concern procedural matters. Under most legislation, the person making the disclosure must make it in good faith and on reasonable grounds. In addition, the information must meet one of the following conditions:

- The information is particularly time sensitive, thus not allowing for prior disclosure through internal channels or to designated independent bodies.
- The disclosure must have already been made through regular channels without a satisfactory or timely response having been received.
- A disclosure made internally or to a designated independent body is likely to result in the destruction or concealment of evidence.
- A disclosure through one of these channels would be likely to result in reprisals against the individual making the disclosure.
- There are no designated internal or independent bodies authorised to receive disclosures.[67]

The above mentioned requirements (or close variations thereof) for making disclosures to the media and public at large are found in the legislation of several common law jurisdictions, including the UK, Canada and South Africa. Laws in other states, such as Romania and Norway, however, do not impose the same preconditions and allow disclosures to the media in the first instance, where the "good faith and reasonable belief tests" have been met.[68]

---

[67] United Kingdom, *Public Interest Disclosure Act 1998*, Chapter 23, Section 43g; South Africa, *Protected Disclosures Act 2000*, Section 9; Canada, *Public Servants Disclosure Protection Act*, S.C. 2005, c. 46, Section 16. This approach is also endorsed by the Parliamentary Assembly of the Council of Europe, Resolution 1729 on the 'Protection of "whistle-blowers,"' 29 April 2010, para., 6.2.3.

[68] Romania, *Law on the Protection of Public Officials Complaining About Violations of the Law 2004*; Norway, *Working Environment Act 2005*. Cited in Venkatesh Nayak, *Public Interest Disclosure and Protection to Persons Making the Disclosures Bill 2010: A Comparison with International Best Practice Standards* (New Delhi: Commonwealth Human Rights Initiative, 2011), 7.

4.3 Disclosures to the media by security sector personnel

Disclosures to the media and public at large give rise to particular concern in the context of the security sector. This is primarily due to the highly sensitive nature of some of information held by security sector organisations and the possible damage (including to the capacity and effectiveness of security sector organisations as well as to the public interest more generally) which could be caused by its release. The release of information about operational methods could, for example, compromise prosecutions or give criminals a tactical advantage vis-à-vis the police. Furthermore, as the Australian Parliamentary inquiry on this issue pointed out: "disclosures to the media concerning [...] national security, intelligence and defence could interfere with proper processes of government and in extreme circumstances put lives at risk."[69]

Information disclosed to the public may have implications for human rights. There are several ways in which the right to privacy could be infringed by the disclosure of personal data. A person's right to fair trial could be compromised by the disclosure of information relating to their case. Perhaps most seriously, one can envisage situations where the right to life could be endangered by *inter alia* the disclosure of information pertaining to sources used by police and intelligence agencies, the operational plans of the armed forces or, more generally, by diminishing the overall capacity of the security sector organisations to protect the right to life.

Opponents of allowing those with access to classified or otherwise confidential information to make disclosures of information showing wrongdoing to the media or public at large would likely argue that individuals within security sector organisations are not well placed to judge the possible harm that would arise from the public dissemination of certain information. Indeed, the way that many security sector organisations are structured means that many personnel only have access to "compartmentalised" information and this may make it difficult for them to arrive at a comprehensive picture that takes into account the full impact of their actions in making a public disclosure.

---

[69] Parliament of Australia, House of Representatives Standing Committee on Legal and Constitutional Affairs, *Whistleblower protection,* 162-3.

In view of these considerations, most examples of legislation on protected disclosures (which ordinarily allow disclosures to the media and public at large) do not extend protections to persons making disclosures of classified or otherwise confidential information. In fact, the overwhelming majority of states criminalise such disclosures. In view of this, it is unsurprising that most persons wishing to disclose information showing wrongdoing only turn to the media as a last resort.[70]

Nevertheless, we argue that some protection should be granted to those who disclose information to the media or public at large in strictly limited circumstances. This is the approach taken by the 2012 Draft Australian Public Interest Disclosure (Whistleblower Protection) Bill, which states that whistleblowers who disclose "sensitive defence, intelligence or law enforcement information" to the public must "satisfy themselves, on reasonable grounds, that the public interest in disclosure ... outweighs the public interest in protection..."[71] Similarly, the South African Protection of State Information Bill states that persons who disclose classified information may not be prosecuted if the disclosure reveals criminal activity.[72]

The Tshwane Principles build on this model in Principle 40 by stating that:

The law should protect from retaliation, as defined in Principle 41, disclosures to the public of information concerning wrongdoing as defined in Principle 37, if the disclosure meets the following criteria:

a) *(1) The person made a disclosure of the same or substantially similar information internally and/or to an independent oversight body and:*
   i. *the body to which the disclosure was made refused or failed to investigate the disclosure effectively, in accordance with applicable international standards; or*
   ii. *the person did not receive a reasonable and appropriate outcome within a reasonable and legally-defined period of time.*

OR

---

[70] Parliament of Australia, House of Representatives Standing Committee on Legal and Constitutional Affairs, *Whistleblower protection,* 11.
[71] Parliament of Australia, House of Representatives, *Public Interest Disclosure (Whistleblower Protection) Bill 2012* (Mr. Wilkie). Para. 33
[72] Republic of South Africa, *Protection of Information Bill 2011.* s.41 (c). This provision was in the draft passed in late 2012; this bill has not yet been enacted.

(2) The person reasonably believed that there was a significant risk that making the disclosure internally and/or to an independent oversight body would have resulted in the destruction or concealment of evidence, interference with a witness, or retaliation against the person or a third party;

OR

(3) There was no established internal body or independent oversight body to which a disclosure could have been made;

OR

(4) The disclosure related to an act or omission that constituted a serious and imminent risk of danger to the life, health, and safety of persons, or to the environment.

AND

b) *The person making the disclosure only disclosed the amount of information that was reasonably necessary to bring to light the wrongdoing;*

AND

c) *The person making the disclosure reasonably believed that the public interest in having the information revealed outweighed any harm to the public interest that would result from disclosure.*

Finally, it is worth noting that because many security sector whistleblowers face criminal prosecution, a defence of last resort will, unfortunately, remain a necessity. In this regard, we can turn to Section 15 of the Canadian Security of Information Act, which states that a person is not guilty of an offence pertaining to the unauthorised disclosure of classified or otherwise confidential information if they can demonstrate that they acted in the public interest. A determination of whether any disclosure of information showing wrongdoing is in the public interest can be based on a two part assessment. Firstly, it must be determined that the person acted to disclose information showing wrongdoing falling into one of several categories provided for by law. Secondly, assuming that the whistleblower acted to disclose information falling into a prescribed category, a court must then determine whether the public interest in making such a disclosure outweighed the public interest in non-disclosure. This weighing of the public interest is the approach that was taken by the European Court of Human Rights (ECtHR) in the case of *Guja v. Moldova* and recently reaffirmed in *Heinisch v. Germany*. The court

has stated that it must "weigh the damage, if any, suffered by the public authority as a result of the disclosure in question and assess whether such damage outweighed the interest of the public in having the information revealed."[73]

This was also the approach taken by the Tshwane Principles, which outline a public interest defence in Principle 43, which states that:

a) *Whenever public personnel may be subject to criminal or civil proceedings, or administrative sanctions, relating to their having made a disclosure of information not otherwise protected under these Principles, the law should provide a public interest defense if the public interest in disclosure of the information in question outweighs the public interest in non-disclosure.*

b) *In deciding whether the public interest in disclosure outweighs the public interest in non-disclosure, prosecutorial and judicial authorities should consider:*
   i. *whether the extent of the disclosure was reasonably necessary to disclose the information of public interest;*
   ii. *the extent and risk of harm to the public interest caused by the disclosure;*
   iii. *whether the person had reasonable grounds to believe that the disclosure would be in the public interest;*
   iv. *whether the person attempted to make a protected disclosure through internal procedures and/or to an independent oversight body, and/or to the public, in compliance with the procedures outlined in Principles 38-40; and*
   v. *the existence of exigent circumstances justifying the disclosure*

While this approach has been criticised, we are not convinced that one can definitively state that there are no circumstances in which the disclosure of even these narrow categories of information would be in the public interest.

[73] *Guja v. Moldova* [GC] no. 14277/04, ECHR 2008, para. 76; *Heinisch v. Germany*, no. 28274/08, ECHR 2011, para. 68.

5. Conclusions

Recent events, including the rise of Wikileaks, the trial of Bradley Manning, and the disclosures made to several newspapers by former NSA contractor Edward Snowden have made security sector whistleblowing frontpage news. Setting aside the array of issues raised by his disclosures, however, the fact that Snowden and other recent whistleblowers have gone directly to the media suggests that, in many jurisdictions, legal and institutional frameworks for protected disclosures—particularly as they relate to the security sector—are either inexistent or inadequate.[74]

Furthermore, a number of states, including in the Balkans, are currently considering legislation which has important implications for whistleblowing in the security sector. On a positive note, relatively comprehensive legislation on the protection of whistleblowers recently came into force in the Republic of Korea.[75] On a more worrying note, the South African parliament adopted a bill that, if enacted, would have significant implications for security sector personnel wishing to disclose information showing wrongdoing.[76]

In addition, the importance of whistleblower protections have been increasingly recognised by international organisations and their member states. Indeed, the initial research for this chapter was done in order to inform the drafting of the Global Principles on National Security and the Right to Information (the "Tshwane Principles"). Furthermore, the United Nations Convention Against Corruption requires that states party consider the establishment of "measures and systems to facilitate the reporting by public officials of acts of corruption to appropriate authorities"[77] Similarly, the

---

[74] See, for example
, Stephen Vladeck, "Left out in the cold: the chilling of speech, association, and the press in post-9/11 America," *American University Law Review*, 57 (June 2008).
[75] Kim Dok-Man, "Better Protection for Whistleblowers," *Korea Times,* 12 Feb 2011; Republic of Korea, Act on the Protection of Public Interest Whistleblowers, Act no. 10472, March 29, 2011.
[76] Republic of South Africa, Protection of State Information Bill, [B 6B—2010] as introduced in the National Assembly; Government Gazette No.32999 of March 2010, Minister of State Security, 13 September 2011. For a cogent critique of this bill see, for example, Dario Milo, "Information bill needed - just not this one," *Times Live*, 27 November 2011.
[77] *United Nations Convention Against Corruption*, Adopted by United Nations General Assembly Resolution 58/4. Merida (Mexico), 23 October 2003, Article 8(4).

Parliamentary Assembly of the Council of Europe (PACE), a body which unites parliamentary representatives from all 47 member states of the Council, recently promulgated a *Resolution on the Protection of Whistleblowers* which outlined the elements of appropriate legislation, as well as invited member states to review extant laws with a view to strengthening whistleblower protection throughout Europe (although not specifically in the context of the security sector).[78] Additionally, in 2010, the UN Special Rapporteur on The Protection and Promotion of Human Rights while Countering Terrorism promulgated (at the request of the UN Human Rights Council) a compilation of intelligence services and their oversight. This compilation included specific guidance on disclosures from within intelligence and security services.[79]

This chapter has provided an overview of whistleblower procedures and protections as they apply to security sector organisations such as the police, intelligence and security agencies and the armed forces. We have tried to demonstrate that systems designed to facilitate, investigate and protect the disclosure of information showing wrongdoing by security sector organisations are essential to promoting accountability, transparency and respect for the rule of law in this sector.

We argue that recent events should serve as a catalyst for the development of legal and institutional frameworks that promote and protect the disclosure of information showing wrongdoing. When built in accordance with international good practice, whistleblower protection regimes can achieve these goals while also ensuring that classified and otherwise confidential information is handled properly.

A well-built system for protected disclosures is not only in the interests of the public writ large but also of the security sector itself. First, it should prevent the public release of information which is properly classified or confidential by providing proper channels

---

[78] Parliamentary Assembly of the Council of Europe, Resolution 1729 on the 'Protection of "whistle-blowers,"' 29 April 2010; Parliamentary Assembly of the Council of Europe, Committee on Legal Affairs and Human Rights. "The protection of whistle-blowers," Rapporteur: Mr Pieter Omtzigt, Doc. 12006, 14 September 2009.
See also Recommendation 1916 (2010).

[79] United Nations Human Rights Council, *Compilation of good practices on legal and institutional frameworks and measures that ensure respect for human rights by intelligence agencies while countering terrorism, including on their oversight*, Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin. A/HRC/14/46, 17 May 2010.

through which information showing wrongdoing can be disclosed and investigated. Second, such a system should help to uncover waste, corruption, mismanagement, human rights abuses, criminal activity and other wrongdoing. Such malfeasance is obviously harmful to a security sector organisation on many levels. It may, for instance, leave them open to potentially costly lawsuits, employees may be subject to criminal proceedings, and finite resources may be wasted at a time when budgets are shrinking. Perhaps more harmful is the damage done to organisations' reputations, particularly in the eyes of the public whose support is required if the police, security services and other security sector organisations are to function effectively. Thus, the disclosure, investigation and resolution of wrongdoing are patently in the interests of these organisations, as well as in the interest of the public at large.