

# **Protecting ‘National Security’ Whistleblowers in the Council of Europe: An evaluation of three approaches on how to balance National Security with Freedom of Expression**

In its recent case law, the ECtHR has extended freedom of expression protection to whistleblowers, including those who work for the intelligence and security sector. Thus, contracting parties to the ECHR are required to balance any damage to national security caused by the disclosure, with the public interest in the information revealed, before handing down sanctions to the whistleblower for a breach of official secrecy. The paper will identify, and critically evaluate, three possible approaches to balancing national security with the whistleblower’s right to freedom of expression and the public interest in the disclosure of the information. These approaches are firstly, an absolute ban on external disclosures for intelligence officials; secondly, a broad exemption from criminal sanctions or other forms of retaliation when the interest in the information disclosed outweighs national security concerns; and finally, protection from reprisals provided only for specific disclosures or categories of wrongdoing, which are exhaustively enumerated in the law. It will examine the compatibility of each approach with nascent COE whistleblower protection standards and conclude that the final approach, in spite of its deficiencies, can best guarantee the whistleblower’s right to free speech while ensuring that security is protected.

Keywords: whistleblowers; public disclosure; intelligence community; public interest; Council of Europe

## ***Introduction***

Institutions often fail us. Public or private institutions can go wrong due to maladministration, incompetence or deliberate attempts to abuse power to achieve illegitimate aims. Such instances of misconduct are often revealed through whistleblowers – individuals who in the course of their work come across information relating to wrongdoing and decide to speak out about it.<sup>1</sup> Such individuals have begun to enjoy protection from retaliation on an international and regional level under freedom of expression provisions in recognition of the fact that in certain cases, the public interest (PI) in the disclosure of certain information can be so compelling as to outweigh a legally binding duty of confidence.<sup>2</sup> Whistleblowers who work for the security or intelligence sector however, remain disadvantaged under this burgeoning protection scheme. In both the US and the UK for instance, individuals from the intelligence world<sup>3</sup> who have proceeded to unauthorised disclosures of wrongdoing, have been met with severe penalties and prosecutions<sup>4</sup> more akin to ‘spies committing treachery’.<sup>5</sup> National security whistleblowers are in many cases ‘separate and immune’<sup>6</sup> from domestic whistleblower protection laws<sup>7</sup> and are instead usually expected to rely exclusively on internal procedures provided by the executive to report instances of wrongdoing they have uncovered.<sup>8</sup>

Recent developments in whistleblower protection however, call for a re-evaluation of the protection provided to the national security whistleblower. In the Council of Europe (COE), the Parliamentary Assembly and the European Court of Human Rights (ECtHR or ‘the Court’) in its recent case law, have been setting standards for the protection of whistleblowers under freedom of expression that have included protection for members of the military and the security and intelligence community.<sup>9</sup> The free speech protection from reprisals that is afforded to good faith whistleblowers in the COE is the result of a balancing exercise between the public interest in disclosure and the public interest in maintaining secrecy. When the former outweighs the latter, restrictions to the whistleblower’s free speech rights cannot be justified, if the whistleblower acted in good faith.<sup>10</sup> This balancing exercise however, when applied in the context of whistleblowing that affects national security, presents a series of complications. If contracting parties to the European Convention on Human Rights (ECHR) are to take this balancing into consideration in order to secure compliance with the Convention, their secrecy laws pertaining to the unauthorised public disclosure of security related information must be framed in a way that allows them to take into account the possible PI in an unauthorised disclosure before handing down any sanctions to the intelligence official.

It is important to note however, that in spite of these developments on the COE level, whistleblower protection legislation is a rarity among European states. In the European Union for instance, only four states<sup>11</sup> have comprehensive whistleblower protection laws, a further 16 have only ‘partial provisions and procedures’<sup>12</sup>, while the remaining states have no form of protection for whistleblowers. The situation for intelligence sector employees is worse, as the framework for their protection remains entirely inchoate, even among the EU and COE member states with more advanced whistleblower protection frameworks. For instance, the United Kingdom’s Public Interest Disclosure Act 1998 excludes members of the Security and Intelligence community,<sup>13</sup> while in Sweden, the general rule that any employee in the public or private sector can pass on information to the media, is not applicable in relation to official secrets and national security information.<sup>14</sup> Similarly, the Romanian Whistleblower Protection Act of 2004 provides particularly broad protection from retaliation to government employees who blow the whistle, however penalties under official secrets legislation in relation to security-sensitive disclosures have been passed down to whistleblowers.<sup>15</sup> Furthermore, some states do not clearly differentiate between the disclosure of state secrets and acts of espionage.<sup>16</sup> For instance, while Swedish legislation makes a clear distinction between the two, by requiring the involvement of a foreign power for the commission of espionage,<sup>17</sup> the UK’s Official Secrets Act 1989 simply penalizes any public disclosure of information for members of the security and intelligence community.<sup>18</sup> Thus, while whistleblower protection for security sector employees is virtually nonexistent, COE member states have robust legislation penalizing the disclosure of state secrets.<sup>19</sup> This varies in forms, especially in relation to how an ‘official secret’ is defined.<sup>20</sup> However, national security consistently appears as a reason to bar disclosure,<sup>21</sup> and coupled with the lack of whistleblower protection for security sector employees, creates an almost impenetrable fortress of secrecy in security matters.

This lack of standards for whistleblower protection in general on the domestic level, prompted the COE Committee of Ministers to release a recommendation<sup>22</sup> encouraging member states to adopt whistleblower protection legislation that allows for a balancing of the public interest in non-disclosure, with the public interest in an informed citizenry. Therefore, what the paper aims to explore, is how secrecy laws or whistleblower protection instruments can incorporate this balancing exercise in order to protect security sector whistleblowers and thus to secure the compatibility of their legislation with freedom of speech standards on the one hand, while ensuring that national security will not be compromised on the other. The

paper identifies three possible avenues for this public interest exercise to be included in the law.

The first approach considers public disclosures, to the media for instance, as incompatible with the role of the intelligence official. It thus altogether disposes of the balancing exercise between the interest in disclosure of the specific information and national security. Consequently, this approach does not require proof of damage to security interests in order to justify retaliation against the whistleblower. In order to ensure the compatibility of such a law with emerging COE freedom of expression standards, the paper argues that a robust system that would permit internal disclosures to official mechanisms for raising concern would be required. If these mechanisms were genuinely independent of the line management chain and could ensure that individuals approaching them would be protected and that their concerns would be effectively addressed, free speech restrictions to public whistleblowers could be justified. The paper will argue however, that such internal mechanisms have their inherent limitations and the COE standards allow for public disclosures even when such mechanisms exist in specific circumstances that will be examined in detail. Thus, an absolute ban on external reporting would be difficult to reconcile with ECHR freedom of expression standards.

The second approach would be for the law to include a rebuttable presumption that public disclosures from intelligence officials are damaging to national security. If the whistleblower was nonetheless able to prove that, as a means of last resort, the interest in publicly disclosing the information outweighed security concerns, protection would be provided. While this approach would require an *ad hoc* assessment of whether any freedom of expression restrictions that the whistleblower experienced were justified based on the damage caused by the disclosure, the lack of a definition as to what would constitute wrongdoing could result in ‘opening the floodgates’ and in allowing overzealous intelligence sector employees to make assessments on particularly sensitive national security issues, thus ‘usurping’ the role of their superiors. If the intelligence official’s duty of confidentiality was conditional in this sense, the intelligence services would not be able to function effectively, and whistleblowers would face the risk that their own interpretation of the public interest, a notoriously nebulous concept, would not be confirmed by the courts.

The final approach includes specific definitions or categories of wrongdoing that would allow the whistleblower to proceed to public disclosures as a means of last resort, either in the form of specific exemptions to secrecy or as categories of protected disclosures in a whistleblower protection instrument. This approach, where the balancing exercise

between national security and the interest in disclosure is enshrined in law, allows whistleblowers a greater degree of certainty that their disclosures will be protected and ensures that they will not proceed to arbitrary PI assessments. However, this has the drawback that whistleblower protection becomes conditional on the generosity of lawmakers in their interpretation of the public interest in the law. Therefore, if lawmakers follow a particularly narrow approach, there is a risk that whistleblowers' free speech rights will not be upheld. Furthermore, the lack of consensus on the international level as to which specific disclosures would be deemed important enough to outweigh national security concerns and allow for public disclosures, would make the implementation of such a system questionable as to its feasibility in the security sector. However, the paper will conclude that this approach offers the most reasonable solution to the issue at hand, and along with strengthened regional standards on whistleblower protection and vigilance on behalf of the judiciary, would provide concrete protection to whistleblowers while ensuring that security concerns are adequately addressed.

Before proceeding with the examination of each of these approaches and their impact on whistleblowers' free speech rights, it is necessary to examine how the freedom of expression of whistleblowers has been protected on the COE level, followed by a short analysis of how the whistleblower becomes, in essence, an assessor of the PI when deciding to proceed to a public disclosure. The paper will then proceed to examine the aforementioned approaches before providing some thoughts on the status of the intelligence official whistleblower.

### ***1) Protection for Whistleblowers in the COE***

Free speech in contracting parties to the Convention is largely informed by Article 10 of the ECHR and the case law of the ECtHR, which domestic courts are expected to take into account when deciding on cases that involve human rights.<sup>23</sup>

When faced with the challenge of assessing whether a restriction to a right is in line with Convention standards,<sup>24</sup> the Court will examine whether the measure that interferes with the right is prescribed by law and whether it is 'necessary in a democratic society'.<sup>25</sup> This requires the state to prove that 'action taken is in response to a pressing social need, and that the interference with the rights protected is no greater than is necessary to address that pressing social need'.<sup>26</sup>

Articles of the Convention that provide for restrictions to rights are to be narrowly construed, however, states enjoy 'a certain but not unlimited margin of appreciation in the

matter of the imposition of restrictions’.<sup>27</sup> The margin of appreciation doctrine, which appears prominently in national security related cases, maintains that state parties are ‘entitled to certain latitude in resolving the inherent conflicts between individual rights and national interests’.<sup>28</sup> This translates in practice to a ‘judicial self-restraint’<sup>29</sup> – at times significant – on the part of the ECtHR.

In relation to state secrecy, the ECtHR has recognised in its case law that ‘a consensus appears to exist among the member States of the Council of Europe on the need for appropriate criminal sanctions to prevent the disclosure of certain confidential items of information’.<sup>30</sup> It is also common practice for intelligence officials to sign agreements that they will never reveal or publish any information relating to their work in the Services, without seeking prior authorisation.<sup>31</sup> However, the COE Parliamentary Assembly, in Resolution 1551 (2007), called on the Court ‘to find an appropriate balance between the state interest in preserving official secrecy on the one hand, and freedom of expression [...] and society’s interest in exposing abuses of power on the other hand’.<sup>32</sup> In a similar vein, Resolution 1507 (2006) had called for member States to ‘ensure that the laws governing state secrecy protect the whistleblowers, that is persons who disclose illegal activities of state organs from possible disciplinary or criminal sanctions’.<sup>33</sup> The Assembly has also consistently argued that ‘[c]rimes such as murder, enforced disappearances, torture or abduction committed by state agents do not deserve to be protected as “state secrets”’.<sup>34</sup> It was Resolution 1729 (2010) on the protection of whistleblowers however, that went further to encourage member states to adopt whistleblower protection legislation for individuals who in good faith ‘sound an alarm in order to stop wrongdoings that place fellow human beings at risk’.<sup>35</sup> The Resolution included members of the security services and armed forces in its ambit of protection.<sup>36</sup> In defining which disclosures should enjoy protection the Resolution provided that:

The definition of protected disclosures shall include all bona fide warnings against various types of unlawful acts, including all serious human rights violations which affect or threaten the life, health, liberty and any other legitimate interests of individuals as subjects of public administration or taxpayers.<sup>37</sup>

It urged state parties to adopt whistleblower legislation that would ‘protect anyone who, in good faith, makes use of existing internal whistle-blowing channels from any form of retaliation’.<sup>38</sup> Thus it is safe to deduce that internal mechanisms are viewed as the initial

avenue for whistleblowers to raise concern. The resolution however, went further to stress that:

[W]here internal channels either do not exist, have not functioned properly or could reasonably be expected not to function properly given the nature of the problem raised by the whistle-blower, external whistle-blowing, including through the media, should likewise be protected.<sup>39</sup>

Therefore, the mere fact that internal whistleblowing mechanisms exist does not suffice to argue that an absolute prohibition on external reporting can be justified. This view was reinforced through the Committee of Ministers recommendation to COE member states, which noted that ‘the individual circumstances of each case will determine the most appropriate channel’<sup>40</sup> for raising concern.

The view that alerting the media should be a viable avenue even for national security whistleblowers was further solidified in the COE’s Parliamentary Resolution 1838 (2011), which provided that:

The media play a vital role in the functioning of democratic institutions, in particular by investigating and publicly denouncing unlawful acts committed by state agents, including members of the secret services. They rely heavily on the co-operation of “whistle-blowers” within the services of the state. The Assembly reiterates its calls for adequate protection...for whistleblowers.<sup>41</sup>

Similarly, Resolution 1877 (2012) provided that in relation to secrecy laws, ‘member States must not curtail the right of the public to be informed by restricting the right of individuals to disclose information of public concern, for example by applying...national security and anti-terrorist laws in an overly broad and non-proportional manner’.<sup>42</sup> Finally, Parliamentary Assembly Resolution 1954 (2013), provided 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’.<sup>43</sup> Applicable procedures would therefore refer to the use internal mechanisms when these are available and public disclosures only in cases where these mechanisms fail.

Turning to the Court, the primacy of free speech in a democratic society is well established in the ECtHR case law.<sup>44</sup> For the ECtHR, the function of the press as a “public watchdog” is central to a democracy,<sup>45</sup> and ‘the national margin of appreciation is limited when the author of the expression in question is a journalist’.<sup>46</sup> Press freedom has indirectly protected anonymous whistleblowers, as the Court has consistently held that compelling a journalist to reveal the source of an information leak constitutes a free speech violation.<sup>47</sup> However, in more recent cases, Article 10 protection has not been limited to protecting the dissemination of leaked information through the press, but was extended to include the source of the leak, the good faith whistleblower.

The landmark case of *Guja v. Moldova*<sup>48</sup>, was the ‘first to deal explicitly with the practice of whistleblowing’.<sup>49</sup> In *Guja*, the ECtHR allowed for Article 10 protection for whistleblowers by asserting that ‘the interest which the public may have in particular information can sometimes be so strong as to override even a legally imposed duty of confidence’.<sup>50</sup> In the case of *Bucur and Toma v Romania*,<sup>51</sup> the ECtHR examined PI disclosures by intelligence officials. The Court seemed to differentiate between leaks of state secrets with no discernible PI<sup>52</sup> (where states retain a wide margin of appreciation in assessing whether their release could damage national security)<sup>53</sup> and whistleblowing in the public interest. The Court held that retaliation against a good faith whistleblower who publicly disclosed instances of illegal surveillance by the Romanian services, after unsuccessfully attempting to address the issue using internal means, was in fact a violation of Article 10. The national security arguments against disclosure in *Bucur*, led the Court to argue that protecting national security cannot come at the price of destroying democracy<sup>54</sup> and it proceeded to criticise the domestic courts for not taking into account the applicant’s arguments relating to the public interest of the information disclosed.<sup>55</sup>

Before proceeding to examine how these developments could affect secrecy legislation in the Contracting Parties to the ECHR however, it is worthwhile to briefly examine the process under which the whistleblower, by deciding that certain information is in fact deserving of exposure, becomes in fact an assessor of the PI. By conducting a PI test to ascertain whether the interest in releasing the information at hand outweighs competing security considerations, national security whistleblowers become engaged in a complex balancing exercise, the outcome of which is not necessarily objective.

## ***2) The whistleblower as an assessor of the Public Interest***



The paper submits that an act of an unauthorised public disclosure can be further analysed into a two - step process. Initially, the whistleblower makes an evaluation that certain information he or she has come across relates to wrongdoing.<sup>56</sup> Subsequently, the whistleblower decides, after finding that an internal report would be ineffectual, that it would be beneficial to make this instance of misconduct public. Both these steps however, contain an assessment that relates to the public interest.

In the first step, according to the whistleblower's understanding, there is a specific activity of an organisation that contravenes the PI. In the national security context, such a balancing exercise, when conducted by the whistleblower, is fraught with dangers. Although in some cases it is self-evident that the information the whistleblower comes across relates to wrongdoing – for instance where there is clear evidence of corruption or state complicity in gross human rights violations – this is not always the case. In the context of national security especially, the work of the intelligence community or the war against terrorism, it may not be simple for the potential whistleblower to discern between legitimate conduct of a public authority, and wrongdoing.<sup>57</sup> The services, by their nature, infringe on human rights, namely the right to privacy protected under Article 8 ECHR, when they monitor communications for instance in order to collect intelligence.<sup>58</sup> For a whistleblower to ascertain whether specific instances of such monitoring constitute misconduct, he or she must perform a balancing exercise to assess whether in these 'suspicious' cases the intelligence agency is acting within the remit of the law or not. Thus, a PI balancing exercise between security and the privacy of the monitored individual must take place before the whistleblower decides to proceed with a disclosure.

The second step involves a decision on whether the perceived wrongdoing is so severe as to warrant a public disclosure. The whistleblower therefore decides to disclose the information in an act that in fact 'overrides the judgment of the executive authority'.<sup>59</sup> This means that the whistleblower asserts, contrary to the judgment of his or her superiors, that the PI will be best served by full disclosure of the information at hand and that this interest outweighs conflicting interests in security.<sup>60</sup> Although the decision to 'go public' could in many cases be motivated by the fact that the whistleblower was unable to address the issue using less extreme measures, an assessment of the PI is required, as the whistleblower would be reluctant to breach his or her duty of confidentiality to reveal information that is trivial and of little importance to the public discourse. As Morse notes, 'not all violations of law are equally important to make public'.<sup>61</sup> Therefore the balancing exercise between the interest in

security and the interest in the disclosure is in such circumstances entrusted to the individual whistleblower.

Due to the PI being a particularly nebulous concept which lacks a concrete and universally accepted definition that can be applied in every case,<sup>62</sup> it is an arduous task for the whistleblower to assess whether this evaluation and judgment that leads to a disclosure is indeed in the PI.<sup>63</sup> This could result in problems when granting free speech protection, as any restrictions to the whistleblower's free speech that are due to damage caused to national security by the disclosure, could be justified under Article 10 (2). Therefore, it is vital for secrecy laws or whistleblower protection instruments pertaining to national security whistleblowers, to take this balancing exercise into account and to examine ways to protect the whistleblower while ensuring that overzealous employees are not encouraged to proceed to complicated PI and national security assessments that result in harmful disclosures.

The question that the paper aims to answer therefore, in relation to the intelligence community whistleblower, is how official secrecy legislation can be framed in light of the recent developments in whistleblower protection mentioned above, in order to ensure firstly, that the whistleblower's assessment on the PI is less of an instinctual process, and secondly, that security is not harmed to a disproportionate extent when weighed against the public interest in disclosure.

After these clarifications the paper will proceed to examine the first possible avenue for secrecy legislation to be framed.

### ***3) The first approach: A blanket ban on disclosures***

The first method to frame secrecy legislation or confidentiality agreements of the intelligence official seeks to exclude discussion of a possible PI in public disclosures, by using criminal law or other retaliatory measures to prosecute those who proceed to any unauthorized disclosures of information. This approach is premised on the idea that it is the act of publicly disclosing security related information *itself* that is contrary to the PI, regardless of whether or not the specific disclosure actually endangered national security.<sup>64</sup> Furthermore, the ECtHR has held that information relating to security and intelligence can legitimately be withheld from the public.<sup>65</sup> This is the system currently favoured by the Official Secrets Act 1989 (OSA 1989) in the UK, for instance which does not allow for public disclosure of information by members of the Intelligence and Security Community, even if it relates to wrongdoing.<sup>66</sup> The OSA 1989 does not include a *damage test* for intelligence officials, which means that the prosecution is not required to prove that there was some damage caused to

national security or other state interests in order to hand down penalties against the whistleblower under criminal law.<sup>67</sup> Furthermore the act does not include a PI defence, which would allow the whistleblower to argue that the public interest in disclosure outweighs the public interest in security. Thus, the irrebuttable presumption that disclosures emanating from the Services are damaging<sup>68</sup> results in prohibiting the judiciary from making an ad hoc assessment of the national security considerations that could be endangered by a specific disclosure, in order to assess the legitimacy of the free speech restriction.

For those supporting this line of argument, the role of the intelligence official should be limited to providing support to the government of the day and not to assume the role of an ‘impartial umpire’ in political disputes.<sup>69</sup> The work of civil servants in general requires them to support and not hinder the government of the day and thus they assume a particularly strong duty of loyalty.<sup>70</sup> Furthermore, since for intelligence officials ‘their official job duty is protecting the country’s national security interests’,<sup>71</sup> more stringent free speech restrictions are permissible. This approach ensures that the whistleblower will not proceed to PI assessments, particularly in issues that touch upon the security of the state. An absolute restriction on disclosures relies on the idea that the interests of maintaining public confidence in these institutions, the fact that such disclosures carry with them a particularly strong credibility, and the heightened duty of secrecy of intelligence officials, all outweigh any potential benefit from a public disclosure.<sup>72</sup> Thus the value of the information disclosed to the PI is not part of the proportionality equation, and any information, however trivial, when disclosed can justify criminal sanctions or other forms of retaliation if the authorities decide to prosecute. Thus the ‘balancing exercise’ of the interest in the information and national security is altogether discarded as ‘the protection of secrets is synonymous with the public interest’.<sup>73</sup>

This approach seems to be irreconcilable *prima facie* with the established COE whistleblower and free speech standards examined above. However, the fact that *public* whistleblowing to the media is protected only when more discreet means of remedying the situation are not available to the whistleblower,<sup>74</sup> could provide contracting parties with the necessary justification to ban external disclosures. If a state chooses to follow such an approach in order to secure the compatibility of the law with free speech, it would have to counterbalance the absolute ban on external disclosures by establishing a robust system of independent and effective internal mechanisms, where whistleblowers could report their concerns and be protected from reprisals while also be assured that the issues they have raised will be addressed appropriately.<sup>75</sup>

The exclusive reliance on internal mechanisms or official channels of reporting however can be said to have significant drawbacks. Sagar argues that internal whistleblowing carries the danger that the wrongdoing may remain unaddressed. As he stresses, ‘senior officials may ignore or suppress a whistleblower’s complaint in order to hide their complicity or to avoid a scandal’,<sup>76</sup> an internal report could leave the whistleblower without ‘external support in the event that her colleagues and managers retaliate against her’,<sup>77</sup> and finally, using official channels without external pressure ‘could provide wrongdoers with the opportunity to destroy incriminating evidence’.<sup>78</sup> Internal reporting ‘may also result in superficial fixes without deep reform’,<sup>79</sup> fixes meant to placate the whistleblower but lacking in bringing about genuine results to rectify the misconduct. Research into whistleblowing has also consistently shown that external whistleblowing has been more successful in eliciting change.<sup>80</sup>

Relying on the ECtHR case law,<sup>81</sup> one could argue that the existence of effective internal mechanisms that be approached by whistleblowers without fear of retaliation would negate the need for a whistleblower to approach the media. However, in recognition of the inherent limitations of official reporting channels, the Court has found the fact that such mechanisms are in place does not suffice to justify an absolute ban on internal disclosures. If the nature of the information at hand made it unlikely for internal mechanisms to respond appropriately, if the internal mechanisms have a history of not addressing instances of such internal whistleblowing, or if they refuse to examine the whistleblower’s allegations, external disclosures are permitted under the ECtHR whistleblowing protection regime.<sup>82</sup> In *Heinisch* and *Bucur* for instance, the whistleblowers had approached their superiors to report the illegal activity they had uncovered, but no concrete action was taken to address the issue. When they subsequently proceeded to a public disclosure they were provided with free speech protection.<sup>83</sup> Therefore, even if such mechanisms exist, they do not suffice to bar<sup>84</sup> the whistleblower from proceeding to a public disclosure and courts from proceeding the ad hoc test of whether they functioned properly in that particular instance and whether the disclosure was in the PI. The first approach therefore, does not provide an adequate solution to the problem of balancing the interests of security and disclosures.

**4) *Second approach: The introduction of a public interest test or defence where wrongdoing is not defined in the legislation***

As the paper has argued, the lack of a PI defence in a contracting party’s secrecy legislation, would make such legislation suspect as to its compatibility with free speech. This part seeks

to discuss how the inclusion of a PI exception to secrecy would affect national security whistleblowers.

Supporters of such an approach argue that official secrecy laws should make for an exception for disclosures emanating from a breach of secrecy that are in the PI.<sup>85</sup> This would allow the intelligence official whistleblower that is facing criminal proceedings for an unauthorized disclosure for instance, to employ a PI defence, and to argue that the interest in the disclosure outweighs the interest in keeping the information secret. Such a defence, which would exonerate national security whistleblowers where they could prove their disclosures were in the PI, would also ensure that the state was in line with freedom of expression standards on whistleblower protection. An example of this approach can be found in Canada, where the Security and Information Act 1985<sup>86</sup> provides that ‘no person is guilty of an offence ... if the person establishes that he or she acted in the public interest’.<sup>87</sup> The Act does not contain a definition of wrongdoing but allows judges to make assessments on whether to grant protection based on the whistleblower’s conduct and good faith, the gravity of the reported offence, the PI in the disclosure and the possible harm it caused.<sup>88</sup> This approach has the added benefit that it allows for a future expansion of the understanding of the types of conduct that constitute wrongdoing, as courts can take into account novel developments without being restricted to a stringent definition of wrongdoing in the law. Similarly in Slovenia, while there is no specialised whistleblower protection instrument, public and private employees are protected for reporting ‘all forms of illegal or unethical behaviour’.<sup>89</sup>

Such a system would require courts to balance the whistleblower’s free speech rights and the public interest in the information disclosed on the one hand, with the potential harm the disclosure may cause to national security on the other, by applying the test of proportionality. Since proportionality ‘seeks to police the justification of state interference with human rights’,<sup>90</sup> it would thus require courts to consider whether any retaliation against a security whistleblower could be defended based on the damage caused to national security by focusing on the content of the disclosure. As the ECtHR has stressed, ‘the Court must look at the “interference” complained of in the light of the case as a whole and determine whether the reasons adduced by the national authorities to justify it are relevant and sufficient’.<sup>91</sup>

In order to gain a better understanding of how such a PI defence would work in practice for the national security whistleblower, it is worthwhile to examine the case law of the ECtHR with regards to whistleblower protection and disclosures in the public interest in general. The Court has provided a useful illustration of how the balancing of the interest in

the disclosure and competing concerns that favour non - disclosure can be exercised, when assessing whether there has been a freedom of expression violation.

In *Guja*, the ECtHR held that the PI involved in the information disclosed is a determining factor in assessing the proportionality of an interference with a whistleblower's free speech rights.<sup>92</sup> The Court took a broad approach in its interpretation of the PI in this instance, by arguing that 'in a democratic system the acts or omissions of government must be subject to the close scrutiny not only of the legislative and judicial authorities but also of the media and public opinion'.<sup>93</sup> In assessing whether freedom of expression protection would be extended to the applicant in this particular case, which involved a public disclosure of information that showed evidence of political interference in the administration of justice from the Moldovan Prosecutor General's Office, the ECtHR proceeded with the usual proportionality test. In order to make the calculation on whether the disclosure had an important benefit to the public at large, the Court looked into the background of the disclosure and the overall political context under which it was made<sup>94</sup> before concluding that '[t]here is no doubt that these are very important matters in a democratic society which the public has a legitimate interest in being informed about and which fall within the scope of political debate.'<sup>95</sup> In the view of the Court these concerns overrode the interests in maintaining public confidence in the Prosecutor General's Office.<sup>96</sup>

In *Bucur and Thoma v Romania*, a case concerning the disclosure of information by a member of the Romanian security services to a newspaper, the ECHR held that 'the general interest in the disclosure of information revealing illegal activities ... was so important in a democratic society that it prevailed over the interest in maintaining public confidence in that institution'.<sup>97</sup> In *Voskuil v. Netherlands* the court stressed that 'in a democratic state governed by the rule of law the use of improper methods by a public authority is precisely the kind of issue about which the public has the right to be informed',<sup>98</sup> while in *Heinisch* it argued for an even broader understanding of the PI by stating that 'there is little scope under Article 10 § 2 of the Convention for restrictions on debate on questions of public interest'.<sup>99</sup> Similarly, in *Dupuis*, the ECtHR took into account the fact that, in France, the revelation of extensive wiretapping of political figures in the media, revealed in a book published by two journalists, had already 'aroused a considerable degree of emotion and concern among public opinion'<sup>100</sup>. Thus, the interest already expressed in France over the revelations was a factor to be considered by the ECtHR in its balancing of the interest in disclosure with competing interests.

It is important to note that proof of the Court's case-by-case approach is found in the fact that the circumstances of every contracting party are taken into account during the proportionality test when assessing the public interest in the disclosure. This is prevalent in issues concerning national security. As Cameron observes, security in the COE is 'both dynamic and relative: what "vulnerability" is will vary from state to state and from time to time'.<sup>101</sup> In *Bucur* for instance, the Court stressed that illegal surveillance by the security services was undeniably a matter of public interest,<sup>102</sup> especially in a state that had experienced extensive surveillance under the previous communist regime. Thus, Romania's historical past was viewed as a contributing factor to accept that there was a pressing PI need in the disclosure, a PI that was viewed as compelling enough to override the intelligence official's duty of secrecy.

This type of assessment, on a case-by-case basis, seems to be the optimum way for domestic courts to establish the proportionality of an interference with free speech, in cases where a national security whistleblower has experienced retaliation. However, when examined from the viewpoint of domestic legislation regarding national security, whistleblowing and official secrecy, a 'general' PI exception to the duty of confidentiality, which does not define in a more broad or narrow manner what disclosures would be in the public interest and would outweigh security considerations, could result in jeopardising national security and the safety of the whistleblower. Without interpretation or guidelines of what the PI is, such legislation would not provide any assurances to the potential whistleblower that their disclosures will be protected. In political terms, the PI is a highly divisive standard. What recent national security related disclosures have confirmed is that "people disagree fundamentally over what the public interest is",<sup>103</sup> as evidenced by the fact that whistleblowers are, in many cases, simultaneously labelled as heroes or traitors.<sup>104</sup> Thus, when the whistleblower becomes an assessor of the PI, there is no guarantee that the courts will confirm his or her interpretation of the concept.<sup>105</sup>

Such disputes, when transferred to the context of a disclosure emanating from the intelligence community, can undermine national security. If the whistleblower's disclosures are the result of an instinctual response that perceived wrongdoing should be reported in the PI, there is no certainty that irreparable damage will not be caused. It would in fact be impossible for the intelligence community to function effectively under such an environment, where PI decisions on disclosure are made at every level by any and every employee with access to information.

Furthermore, even in cases where one could argue that whistleblowers were prudent in their interpretation of the PI, it is questionable whether this would be accepted by the judiciary. Domestic courts have, to a great degree, shown reluctance to question the executive on matters of national security. As Popelier and Van De Heyning note, constitutional and supreme courts in Europe, tend to ‘readily accept public safety and security concerns proposed by public authorities as legitimate objectives with a considerable weight, without scrutinizing the danger ... threats actually pose’.<sup>106</sup> Thus, a great degree of deference is given to decision-makers or the executive in assessing which information should remain secret.

As many proponents of whistleblowing propose, a way to overcome these potential problems is to set the threshold for protection based on whether the whistleblower acted under the ‘reasonable belief’ that he or she was uncovering wrongdoing that was in the PI.<sup>107</sup> Protection, it is argued, should also cover disclosures made ‘in honest error’<sup>108</sup> when the information on wrongdoing that is publicly revealed is inaccurate but the whistleblower acted in good faith with the disclosure. This has the benefit of disengaging protection from whether the information was in fact in the PI. Yet, when applied to national security whistleblowers, it could be said to create more problems than it solves. Firstly, setting the bar at reasonable *belief* that wrongdoing was committed would require the whistleblower to proceed to a more thorough examination of the wrongdoing he / she is alleging was committed. This in many cases would not be possible to do or could potentially be harmful to the whistleblower and could thus further dissuade concerned individuals from proceeding to the disclosure. As Lewis proposes, requiring reasonable *suspicion*, as opposed to reasonable *belief*, would be a better approach as ‘the great advantage of this would be that it would highlight the fact that it is the recipient's job to investigate concerns and not that of the potential whistleblower’.<sup>109</sup> However, it is questionable that in the context of national security whistleblowers this approach would be realistic. Keeping in mind the heightened demands for secrecy the services function under,<sup>110</sup> extending free speech protection to disclosures where the concerns for national security would outweigh the interest in disclosure would be difficult to reconcile with Article 10(2) ECHR. These are the dangers inherent in legislation that would not enumerate specific areas of concern, which would guide the whistleblower during his or her PI assessment.

Thus, providing protection for PI disclosures without defining the PI in the law, ensures that the law will allow for a balancing of national security and competing interests on a case by case basis and thus will not collide with free speech standards. At the same time however, such an approach has the potential to prove more damaging for both the



whistleblowers, who will have to navigate the nebulous concept that is PI without guidance, and also to national security as the duty of secrecy will become conditional on the PI assessments of any employee that handles confidential information.

This leads us to the examination of the third approach to whistleblower protection / official secrecy laws.

**5) *Third approach: A list of specific PI disclosures contained in the whistleblower protection instrument.***

Providing whistleblower protection for only specific types of disclosures enumerated in the whistleblower protection instrument or in official secrecy legislation has the benefit of giving the whistleblower greater certainty that his/her disclosure will be perceived to be in the PI, a PI that will override competing security concerns. In this approach, the balancing between national security and the public's right to know is included in the legal instrument and the function of the judiciary is limited to examining whether a specific disclosure falls under one or more pre-determined categories.

The inclusion of a prescribed list of disclosures, especially in relation to national security, raises the obvious and important question of *which* types of wrongdoing should qualify for protection. It is first advisable to examine whether there is an international consensus on how whistleblowing and secrecy laws deal with definitions on wrongdoing and the public interest in disclosures. Second, one must assess whether there are developing international standards on when national security related disclosures would be in the PI. Finally, it should be asked whether nascent ECHR and COE standards on whistleblowing could provide contracting parties with the necessary guidelines to draft their secrecy legislation.

According to Banisar, there are more than 30 countries around the world that have adopted some form of whistleblower protection,<sup>111</sup> and most 'create comprehensive definitions of what constitutes wrongdoing'.<sup>112</sup> Others limit it to one area, usually crimes related to corruption, while others provide protection for the disclosure of 'a wide variety of issues including violations of laws, good practises, and ethics'.<sup>113</sup> Furthermore, due to the fact that 'the definition of "public interest" varies across different jurisdictions',<sup>114</sup> there are no established international standards or a consensus as to what qualifies as a public interest disclosure.<sup>115</sup>

States possess a degree of flexibility in deciding which areas are most important to protect. Circumstances that are specific to certain states seem to play an important part in

deciding which areas of wrongdoing will be included in a whistleblower protection instrument. As Banisar<sup>116</sup> observes, the South African Act ‘includes unfair discrimination’<sup>117</sup> as a category where PI disclosures apply, while the Japanese equivalent ‘specifically names food and health laws, clean air and waste disposal, and personal information laws’.<sup>118</sup> The US approach seems particularly all encompassing<sup>119</sup> as the federal Whistleblower Protection Act of 1989 protects government employees from sanctions for reporting violation of ‘law, rule and regulation’ or ‘gross mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety’.<sup>120</sup> Furthermore, in the US there are whistleblower protection schemes found in laws relating to a more specific context. As Dworkin explains, ‘an individual who reports illegal water pollution, for instance, is protected from retaliation by the Safe Water Drinking Act’.<sup>121</sup> As Banisar observes, there is agreement however in that states ‘typically require that the action is not trivial in nature and has not previously been disclosed or addressed’.<sup>122</sup>

How could such categories of protected disclosures however, be framed in the context of national security? In the search for international standards on the reasons that would allow for public disclosures of wrongdoing in national security cases, Transparency International has made a significant contribution to the discussion in its 2013 International Principles for Whistleblower Legislation by arguing that:

External disclosure (i.e. to the media, civil society organisations) would be justified in demonstrable cases of urgent or grave threats to public health, safety or the environment; if an internal disclosure could lead to personal harm or the destruction of evidence; and if the disclosure was not intended or likely to significantly harm national security or individuals.<sup>123</sup>

In a similar vein, the Tshwane Principles on National Security and Access to Information (2013) attempted to deal with the issue of national security whistleblowers and the balancing between national security concerns and their free speech rights. The Principles were endorsed by the UN and OSCE Rapporteurs on Freedom of Expression and formed the basis for the COE’s Parliamentary Assembly Resolution 1954 (2013) which will be examined below.

The principles provide a more specific list as to which types of wrongdoing could trigger *public* disclosures when left unaddressed by internal mechanisms and would allow for protection based on the whistleblower’s freedom of speech. The list includes violations of

International Human Rights and Humanitarian Law, such as the prevention of torture, violations of the right to life, decisions to use military force or acquire weapons of mass destruction, mass surveillance, mismanagement or waste of funds, constitutional and statutory violations, abuses of power and issues relating to public health, public safety or the environment.<sup>124</sup>

Adapting these principles to the COE level, the Parliamentary Assembly in its 2013 Resolution on National Security and Access to Information stated that an overriding PI can typically be found where the publication of the information in question would make ‘an important contribution to an ongoing public debate, promote public participation in political debate, expose serious wrongdoings, including human rights violations, other criminal offences, abuse of public office and deliberate concealment of serious wrongdoing, ... benefit public health or safety’.<sup>125</sup> The Resolution added that ‘information about serious violations of human rights or humanitarian law should not be withheld on national security grounds in any circumstances’.<sup>126</sup>

The obvious focus of these provisions is the violation of human rights. The reporting of gross human rights violations would in all cases seem to trump national security concerns and allow for the national security whistleblower to be protected from retaliation. The Tshwane principles in particular, are drawn in a way that validates recent high-profile security-related whistleblowing cases,<sup>127</sup> however, they could be viewed as overly ambitious, as one would expect from a document aiming to provide broad international guidelines on whistleblower protection. A strikingly bold step for instance, is the inclusion of decisions on the use of military force as a protected category, where there would be a ‘high presumption’<sup>128</sup> in favour of disclosure. This, according to the Tshwane principles, would include protection for disclosure of ‘information relevant to a decision to commit combat troops or take other military action, including [...] its general size and scope’.<sup>129</sup> Thus according to the Principles, reporting general information on size and scope would suffice, and a disclosure need not contain ‘all of the details of the operational aspects of the military action’<sup>130</sup> to satisfy the PI in accessing the information. Without doubt, disclosing information during the decision-making process leading up to combat would be valuable to the PI if there were deliberate attempts from the executive and the intelligence services to mislead the legislature and the public<sup>131</sup> on the necessity of combat or its rationale. A more realistic approach however, would argue that it would be destructive to make combat related decisions under the glaring eye of publicity and to allow anyone with access to the specific

information to make assessments on which of the operational details could be reported in the PI.

This example of information on the use of military force as a protected category of disclosure, illustrates the fact that the existence of a prescribed list of disclosures does not relieve the whistleblower from the responsibility of proceeding to complicated PI assessments, much like in the second approach we described. Is it feasible to expect every intelligence official to be able to discern which operational aspects of an upcoming or ongoing combat are worth reporting or whether specific ‘suspicious’ conduct constitutes ‘a constitutional or statutory violation’<sup>132</sup> which the Tshwane Principles regard as a legitimate reason for public disclosures? Although this is true of every whistleblower, in security related cases the adverse results of an incorrect assessment are arguably more profound. Consequently, a list of protected disclosures as broad as the Tshwane Principles or the ones cited in Parliamentary Assembly Resolution 1954, can be further criticised for being ambiguous and vague in nature. This is compounded by the fact that, for security whistleblowers it is ‘impossible [...] to obtain independent legal or other advice before making a disclosure’.<sup>133</sup> However, highly specific and unambiguous categories of wrongdoing would have the drawback of being too limited and providing protection that is too narrow and is not adaptable to newer developments.

Thus it is questionable whether, in the realm of the intelligence community, where decisions are made on sometimes fragmented intelligence in a highly compartmentalised environment, this approach in essence manages to overcome the problems of the whistleblower making sensitive PI assessments cited in the second approach we described. Furthermore, it is important to note that since ‘hard’ data, purely factual information, are not always sufficient to make security related decisions, intelligence agencies also have to rely on *speculative* intelligence in order to determine which people ‘are probably or possibly, threatening national security’.<sup>134</sup> This is a highly subjective exercise and a degree of deference to agency decisions is required, because when it comes to striking these balances, the optimum way to deal with a potential threat ‘is not always straightforward, and reasonable people can differ on how to do it’.<sup>135</sup> Thus, this final method to frame secrecy laws does not entirely resolve the dangers that can arise from well-meaning, yet overzealous, national security whistleblowers.

Furthermore, the fact that the principles mentioned above are derived from non-binding instruments means that they can only serve as an indication or suggestion for legislators. Therefore, when allowing the types of wrongdoing that warrant public disclosure as a means

of last resort to be enumerated in the law, whistleblower protection in national security cases becomes conditional on how generous lawmakers will be in their interpretation of the PI in the whistleblower protection instrument or the secrecy law. This problem is not limited to national security whistleblowers. For instance, and in stark opposition to the broad protection provided to federal whistleblowers in the US mentioned above, in France, the French Labour Law code provides protection only for disclosures relating to allegations of corruption.<sup>136</sup> Although corruption is a particularly broad term, such legislation would still preclude a significant number of whistleblowers whose disclosures are arguably in the PI from seeking protection from retaliation. Although the extent to which legislators will agree that certain national security disclosures warrant specific protection can be indicated by their free speech obligations, they would still be permitted great latitude when translating free speech standards for national security whistleblowers into the domestic context.

In spite of these drawbacks however, this seems to be the most reasonable approach for national legislators. To ensure the compatibility of domestic laws with Article 10 without weakening the secrecy that is necessary for the intelligence community to function, there would need to be a strict prohibition on disclosures, with exemptions where the PI would override secrecy requirements, in line with COE and ECtHR free speech standards and COE guidelines; combined with the strengthening of the independence of intelligence oversight bodies and official reporting mechanisms; as well as adequate training of officials as to what the responsible whistleblowing procedures are. Further development of standards in whistleblower protection on the COE level, through the Assembly and the ECtHR, would allow the judiciary in contracting parties to challenge overly restrictive domestic laws that provide for an excessively narrow list of protected public disclosures. It would also ensure that the ECtHR retains its supervisory role in cases where unwarranted retaliatory measures were taken against whistleblowers whose disclosures are not damaging to national security and contain information that makes a significant contribution to the public interest.

### ***Concluding thoughts***

Technological developments and the advent of the digital age have made it significantly easier to leak and share security related information.<sup>137</sup> Therefore, the need to find an appropriate way to balance national security with the public's 'right to know' is more pressing than ever. The paper has attempted to highlight the problems that occur when attempting to regulate national security whistleblower exceptions to state secrecy in a manner that is compatible with emerging freedom of expression standards of the COE. The COE

adheres to the view that whistleblowers are ‘part of society’s alarm and self-repair system, bringing attention to problems before they become far more damaging’,<sup>138</sup> and it has, in recent years, significantly extended free speech protection for unauthorised public interest disclosures. The impact this will have on the domestic context remains to be seen, as courts and legislators will have to grapple with the task of balancing security interests with the need for an informed citizenry. Out of three possible avenues for the PI to be incorporated into secrecy laws or whistleblower instruments, the paper has argued that, in relation to national security, broad categories of wrongdoing must be included in the law to ensure that intelligence officials who proceed to PI disclosures will enjoy free speech protection. This will also allow for greater guarantees that the public interest in the information disclosed will outweigh the potential harm to national security. The judiciary will be vital in ensuring that legislators include a list of protected disclosures that are in line with ECHR demands on restrictions to freedom of expression, while the ECtHR, civil society and the broader international community can continue to establishing standards for balancing of national security with the public accountability of intelligence institutions for their actions. The fundamental role of freedom of expression in combating corruption and wrongdoing must thus be strengthened and not sacrificed at the altar of national security rhetoric in the intelligence community.

## Notes

---

<sup>1</sup> Whistleblowing is ‘the reporting by employees or former employees of illegal, irregular, dangerous or unethical practices by employers’. International Labour Organisation, ‘ILO Thesaurus’, <http://www.ilo.org/thesaurus/defaulten.asp>. Also see Transparency International, ‘International Principles for Whistleblower Legislation’, Report published 5 November 2013, available at [http://www.transparency.org/whatwedo/pub/international\\_principles\\_for\\_whistleblower\\_legislation](http://www.transparency.org/whatwedo/pub/international_principles_for_whistleblower_legislation), OECD, ‘G20 Anti-corruption action plan: Protection for Whistleblowers, Study on Whistleblower Protection Frameworks, Compendium of Best Practices and Guiding Principles for Legislation (2011)’ <http://www.oecd.org/g20/topics/anti-corruption/48972967.pdf> and Lewis David, *A global approach to public interest disclosure: What can we learn from existing whistleblowing legislation and research?* (Cheltenham: Edward Elgar, 2010).

<sup>2</sup> On the United Nations level protection is provided through the UN Convention against Corruption (2003) Article 33. Protection afforded in the Council of Europe will be examined in detail below.

<sup>3</sup> The scope of the paper is limited to individuals who are employed in the intelligence community and the security sector and are bound by secrecy laws or confidentiality agreements relating to the disclosure of intelligence information. For an analysis and definitions of security services and intelligence agencies in the COE context, see European Commission for Democracy through Law (Venice Commission), ‘Report on the Democratic Oversight of the Security Services’ (2007) [http://www.europarl.europa.eu/meetdocs/2009\\_2014/documents/libe/dv/3\\_cdl-ad%282007%29016\\_ /3\\_cdl-ad%282007%29016\\_en.pdf](http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/3_cdl-ad%282007%29016_ /3_cdl-ad%282007%29016_en.pdf).

<sup>4</sup> As in the convictions of David Shayler and Katharine Gun in the UK, Chelsea Manning and Edward Snowden in the USA.

<sup>5</sup> Palmer Stephanie, ‘Tightening Secrecy Law: the Official Secrets Act 1989’, *Public Law*, 1990: 252.

---

<sup>6</sup> Vaughn G. Robert, *Successes and Failures of Whistleblower Laws* (Cheltenham: Edward Elgar Publishing, 2012) 314.

<sup>7</sup> For a thorough examination of the reprisals whistleblowers experience see Alford Fred, *Whistleblowers: Broken Lives and Organizational Power* (Ithaca, NY: Cornell University Press, 2001) and Jubb PB, 'Whistleblowing: A Restrictive Definition and Interpretation', *Journal of Business Ethics* 21 (1999): 77

<sup>8</sup> Vaughn, *Successes and Failures*, 314.

<sup>9</sup> These will be examined in detail in below.

<sup>10</sup> For an analysis of the good faith requirement in the ECtHR case law see Bowers John and others, *Whistleblowing: Law and Practice* (Oxford: Oxford University Press, 2012) paragraph 11.140 .

<sup>11</sup> These are Luxembourg, Romania, Slovenia and the United Kingdom. See Transparency International, *Whistleblowing in Europe: Legal Protections for Whistleblowers in the EU* (Transparency International, 2013) at 10 available at [http://www.transparency.org/whatwedo/publication/whistleblowing\\_in\\_europe\\_legal\\_protections\\_for\\_whistleblowers\\_in\\_the\\_eu](http://www.transparency.org/whatwedo/publication/whistleblowing_in_europe_legal_protections_for_whistleblowers_in_the_eu) .

<sup>12</sup> Ibid.

<sup>13</sup> Employment Rights Act 1996 s43B (3).

<sup>14</sup> Transparency International, *Whistleblowing in Europe* at 14

<sup>15</sup> Article 3 and Article 10 of law No. 51/1991 of 29 July 1991 on official secrecy. For prosecutions of whistleblowers see ECtHR, *Bucur and Toma v. Romania* (App. No. 40238/02, 8 January 2013).

<sup>16</sup> Cameron Iain, *National Security and the European Convention on Human Rights* (The Hague: Kluwer International Law, 2000) 382.

<sup>17</sup> Swedish Criminal Code, chapter 19, sections 5 and 7.

<sup>18</sup> Official Secrets Act 1989 s1.

<sup>19</sup> See COE Parliamentary Assembly, "Fair trial issues in criminal cases concerning espionage or divulging state secrets" 25 September 2006 Report by Christos Pourgourides [http://assembly.coe.int/ASP/Doc/XrefViewHTML.asp?FileID=9149&Language=EN#P391\\_61374](http://assembly.coe.int/ASP/Doc/XrefViewHTML.asp?FileID=9149&Language=EN#P391_61374) .

<sup>20</sup> Ibid at [57] and [58].

<sup>21</sup> Ibid. The report by Rapporteur Pourgourides contains an exhaustive analysis and comparison on the regulation of official secrecy in the COE region in paragraphs [56] – [68].

<sup>22</sup> Recommendation CM/Rec(2014)7 of the Committee of Ministers to member States on the protection of whistleblowers. Adopted by the Committee of Ministers on 30 April 2014, at the 1198th meeting of the Ministers' Deputies.

<sup>23</sup> Foster Steve, 'Are we becoming afraid of free speech?', *Coventry Law Journal* 18 (2013): 93.

<sup>24</sup> Jacobs, White and Ovey, *The European Convention on Human Rights* (Oxford: Oxford University Press, 2010) 312.

<sup>25</sup> Ibid.

<sup>26</sup> Ibid. at 325.

<sup>27</sup> ECtHR, *Silver and Others v United Kingdom*, (Application no. 5947/72; 6205/73; 7052/75; 7061/75; 7107/75; 7113/75; 7136/75, 25 March 1983) at [97]. On the use of proportionality see Rivers Julian, 'Proportionality and variable intensity of review', *Cambridge Law Journal* 65 (2006): 174.

<sup>28</sup> Benvenisti Eyal, 'Margin of Appreciation, Consensus and Universal Standards', *NYU Journal of International Law and Policy* 31 (1998-1999): 843.

<sup>29</sup> Mahoney Paul and Early Lawrence, 'Freedom of Expression and National Security: Judicial and Policy Approaches under the European Convention on Human Rights and Other Council of Europe Instruments' in *Secrecy and Liberty: National Security, Freedom of Expression and Access to Information*, eds. Sandra Coliver et al. (The Netherlands: Kluwer International, 1999) 116. See also Leigh Ian, 'Case Comment: Spycatcher in Strasbourg', *Public Law*, 1992: 203, 200, 203. On the abuse of national security see Arai –Takahashi Yutaka, *The Margin of Appreciation Doctrine and the Principle of Proportionality in the Jurisprudence of the ECHR* (Oxford: Intersentia, 2002) 104, Christophersen Jonas, *Fair Balance: Proportionality, Subsidiarity and Primarity in the European Court of Human Rights* (Brill, 2009), Noorlander Peter, 'Fighting Words – The War on Terror and Media Freedom' in *Freedom of Expression and the Media*, eds. Amos, Harrison and Woods (Netherlands: Martinus Nijhoff Publishers / Brill Academic, 2012) 229. In the Court's case law see ECtHR, *Leander v. Sweden* (App. No. 9248/81, 26 March 1987), ECtHR, *Klass and others v. Germany* (App. No. 5029/71, 6 September 1978), ECtHR, *A. and others v. United Kingdom* (App. No. 3455/05, 19 February 2009).

<sup>30</sup> ECtHR, *Stoll v. Switzerland* (App. No. 69698/01, 10 December 2007) at [155].

<sup>31</sup> Hoffman Paul and Kate Martin. 'United States' in *Secrecy and Liberty: National Security, Freedom of Expression and Access to Information*, eds. Sandra Coliver et al. (The Netherlands: Kluwer International, 1999) 496.

- <sup>32</sup> Council of Europe Parliamentary Assembly, Resolution 1551 (2007) ‘Fair trial issues in criminal cases concerning espionage or divulging state secrets’, 19 April 2007 at [9].
- <sup>33</sup> Council of Europe Parliamentary Assembly, Resolution 1507 (2006) ‘Alleged secret detentions and unlawful inter-state transfers of detainees involving Council of Europe member states’, 27 June 2006 at [19.5.].
- <sup>34</sup> Council of Europe, ‘Call for protection of whistleblowers who reveal state wrongdoing’, 2 October 2013 available at <http://www.assembly.coe.int/nw/xml/News/News-View-EN.asp?newsid=4669&lang=2&cat=8>.
- <sup>35</sup> Council of Europe Parliamentary Assembly, Resolution 1729 (2010) ‘Protection of Whistleblowers’, 29 April 2010 at [1].
- <sup>36</sup> Ibid at [6.1.2.].
- <sup>37</sup> Ibid at [6.1.1.]. For an in – depth analysis of Resolution 1729 see Lewis David, ‘The Council of Europe Resolution and Recommendation on the Protection of Whistleblowers’, (2010) 39 *Industrial Law Journal* 39 (2010): 72.
- <sup>38</sup> Resolution 1729 at [6.2.1.].
- <sup>39</sup> Ibid at [ 6.2.3.].
- <sup>40</sup> Recommendation CM/Rec(2014)7 of the Committee of Ministers.
- <sup>41</sup> Council of Europe, Parliamentary Assembly Resolution 1838 (2011) ‘Abuse of state secrecy and national security: obstacles to parliamentary and judicial scrutiny of human rights violations’, 6 October 2011 at [8].
- <sup>42</sup> Council of Europe, Parliamentary Assembly Resolution 1877 (2012) ‘The Protection of Freedom of Expression and Information on the Internet and Online Media’, 25 April 2012 at [4].
- <sup>43</sup> Council of Europe, Parliamentary Assembly Resolution 1954 (2013) on ‘National Security and Access to Information’, 2 October 2013 at [9.7.].
- <sup>44</sup> See for instance ECtHR, *Handyside v. United Kingdom* (App. No. 5493/72, 7 December 1976), ECtHR, *Steel and Morris v. United Kingdom* (Application no. 68416/01, 15 February 2005), *Lingens v. Austria* (Application no. 9815/82, 8 July 1986), *Vogt v. Germany* (App. No. 17851/91, 26 September 1995).
- <sup>45</sup> ECtHR, *Goodwin v United Kingdom* (App. No. 17488/90, 27 March 1996) at [39].
- <sup>46</sup> Jacobs, White and Ovey, *The European Convention*, 433 and ECtHR, *Prager and Oberschlick v. Austria* (App. No. 15974/90, 26 April 1995) at [38].
- <sup>47</sup> ECtHR, *Financial Times Ltd and Others v UK* (App. No. 821/03, 15 December 2009).
- <sup>48</sup> ECtHR, *Guja v. Moldova* (App. No. 14277/04, 12 February 2008).
- <sup>49</sup> Jacobs, White and Ovey, *The European Convention*, 442.
- <sup>50</sup> *Guja v Moldova* at [74]. This position was reiterated in the subsequent cases of ECtHR, *Heinisch v. Germany* (App. No. 28274/08 21 July 2011) and ECtHR, *Sosinowska v Poland* (App. No. 10247/09, 18 October 2011).
- <sup>51</sup> ECtHR, *Bucur and Toma v. Romania* (App. No. 40238/02, 8 January 2013).
- <sup>52</sup> See for instance ECtHR, *Hadjianastassiou v. Greece* (App. No. 12945/87, 16 December 1992) and ECtHR, *Pasko v Russia* (App. No. 69519/01, 22 October 2010).
- <sup>53</sup> *Hadjianastassiou* at [47].
- <sup>54</sup> *Bucur* at [102].
- <sup>55</sup> Ibid.
- <sup>56</sup> Near and Miceli refer to this step as the ‘triggering event’ and define it as ‘an activity that is considered wrongful, rather than an acceptable but not optimal organizational activity’ in Miceli Marcia and Near Janet, *Blowing the Whistle: The Organizational and Legal Implications for Companies and Employees* (New York: Lexington Books, 1992) 17 (emphasis added).
- <sup>57</sup> For further analysis on this process see Sagar Rahul, *Secrets and Leaks: The Dilemma of State Secrecy* (Princeton: Princeton University Press, 2013) 103-26.
- <sup>58</sup> Venice Commission Report, ‘Oversight of Security Services’, 4.
- <sup>59</sup> Sagar Rahul, ‘On Combating the Abuse of State Secrecy’, *The Journal of Political Philosophy* 15 (2007): 424.
- <sup>60</sup> See also Bok Sissela, ‘Whistleblowing and Professional responsibility’ in *Ethical issues in business: inquiries, cases, and readings*, ed. Tittle Peg (Ontario: Broadview Press, 2000) 70.
- <sup>61</sup> Morse Mika, ‘Honor or betrayal: The Ethics of Government Lawyer Whistleblowers’, *Georgetown Journal of Legal Ethics* 23 (2010): 448.
- <sup>62</sup> Flathman Richard, *The public interest: An essay concerning the normative discourse of politics* (New York: Wiley 1966) 13.
- <sup>63</sup> One could argue that this assessment on the public interest in public disclosure is made by the whistleblower in conjunction with the medium that will publish it.
- <sup>64</sup> See for instance Rimington Stella, *Open Secret* (London: Arrow Books 2002) 186 and Sagar Rahul, ‘Wikileaks and Democracy’, in *Wikileaks and the Consequences: Internet, Media, Politics*, ed. Heinrich Geiselberger (Frankfurt: Suhrkamp) 2010.



---

<sup>65</sup> See ECtHR, *Murray v United Kingdom* (App. No. 14310/88, 28 October 1994), *Vereniging Weekblad Bluf v. The Netherlands* (App. No. 16616/90, 9 February 1995), and ECtHR, *Telegraaf Media Nederland and others v. Netherlands* (App. No. 39315/06, 22 November 2012).

<sup>66</sup> UK Official Secrets Act 1989, s 1 (1). The Espionage Act 1917 in the USA makes for a similar ‘broad and sweeping prohibition’. Vladeck Stephen, ‘The Espionage Act and National Security Whistleblowing after *Garcetti*’ *American University Law Review* 57 (2007-2008): 1534.

<sup>67</sup> See Rogers Ann, *Secrecy and Power in the British State: A History of the Official Secrets Act* (London: Pluto Press, 1997), Lustgarten Laurence and Leigh Ian, *In From the Cold* (Oxford: Clarendon Press, 1994), Moran Christopher, *Classified: Secrecy and the State in Modern Britain* (Cambridge: Cambridge University Press, 2013).

<sup>68</sup> Smith ATH, ‘Security services, leaks and the public interest’ *Cambridge Law Journal* 61 (2002): 515.

<sup>69</sup> UK House of Commons Public Administration Select Committee, ‘Leaks and Whistleblowing in Whitehall: Tenth Report of Session 2008-09’ HC 83 11.

<sup>70</sup> See ECtHR, *Ahmed and Others v. United Kingdom* (App. No. 22954/93, 2 September 1998).

<sup>71</sup> Sasser Jamie: ‘Silenced Citizens: The post-Garcetti Landscape for Public Sector Employees working in National Security’ *University of Richmond Law Review* 41 (2006-2007): 760.

<sup>72</sup> Fenwick Helen, *Civil Liberties and Human Rights* (Oxford: Routledge – Cavendish, 2007) 597.

<sup>73</sup> Freivogel William, ‘Publishing National Security Secrets: The Case For Benign Indeterminacy’, *Journal of National Security Law and Policy* 3 (2009): 98.

<sup>74</sup> *Guja* at [73]. See also ECtHR, *Morissens v. Belgium* (App. No. 11389/85, Commission decision 3 May 1988).

<sup>75</sup> The existence of internal mechanisms was the justification used in *R v Shayler* [2002] UKHL 11 by the Law Lords in the UK to justify the compatibility of the Official Secrets Act with Article 10. The Lords argued that there was no need to examine the efficiency of such mechanisms. This justification seems weak in light of the COE standards that were subsequent to the Shayler judgment, thus putting into question the compatibility of the OSA with free speech. This is the system also currently followed in New Zealand where the particularly broad Protected Disclosures Act 2000 does not cover national security whistleblowers. Security sector employees can only approach an Ombudsman the Inspector-General of Intelligence and Security. Banisar David, ‘Whistleblowing: International Standards and Developments’ in *Corruption and Transparency: Debating the Frontiers between State, Market and Society*, ed. I.E. Sandoval World Bank-Institute for Social Research, UNAM, Washington, D.C. 2011, available at [http://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=1753180](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1753180) 45. In the USA, intelligence officials are allowed to approach the House and Senate Intelligence Committees with national security disclosures under the Military Whistleblower Protection Act 1988, and the Intelligence Community Whistleblower Act 1998. See Fisher, National Security Whistleblowers (Report for the Congressional Research Service, Library of Congress 2005) <http://www.fas.org/spp/crs/natsec/RL33215.pdf> at 45.

<sup>76</sup> Sagar, *Secrets and Leaks*, 133.

<sup>77</sup> *Ibid.*

<sup>78</sup> *Ibid.*

<sup>79</sup> Morse, ‘Honor or Betrayal’, 449.

<sup>80</sup> Near Janet and Miceli Marcia, ‘Organizational Dissidence: The case of Whistle-Blowing’, *Journal of Business Ethics* 4 (1985): 11, Dworkin Terry and Baucus Melissa, ‘Internal vs. External Whistleblowers: A Comparison of Whistleblowing Processes’, *Journal of Business Ethics* 17 (1998): 1295. For a more recent study conducted in the UK, see Public Concern At Work, ‘Report on ‘Whistleblowing: The Inside Story’ found at <http://pcaaw.org.uk/files/Whistleblowing%20-%20the%20inside%20story%20FINAL.pdf> at 5.

<sup>81</sup> *Guja* [80-84], *Heinisch* [72-76]. Also see dissenting opinion in ECtHR, *Kudeshkina v. Russia* (App. No. 29492/05, 14 September 2009).

<sup>82</sup> Resolution 1729 [6.2.3.].

<sup>83</sup> *Heinisch* [72-76], *Bucur* [97].

<sup>84</sup> An ideal internal mechanism would include: “a clear statement that malpractice is taken seriously in the organisation... respect for the confidentiality of staff raising concern... an opportunity to raise concern outside the management structure and effective follow up mechanisms that will provide the whistleblower with information on how their concern has been addressed”. See Dehn Guy, ‘Whistleblowing and Integrity: a New perspective’ found at <http://www.cfoi.org.uk/pdf/corruptiongd.pdf>

<sup>85</sup> Palmer for instance argues that if internal mechanisms fail, intelligence officials should be permitted to use a public interest defence if prosecuted. Palmer, ‘Tightening Secrecy Law’, 252.

<sup>86</sup> (R.S.C., 1985, c. O-5)

<sup>87</sup> *Ibid.* s.15.

<sup>88</sup> *Ibid.*

<sup>89</sup> Transparency International, *Whistleblowing in Europe* at 79.

- <sup>90</sup> Legg Andrew, *The Margin of Appreciation in International Human Rights Law: Deference and Proportionality* (Oxford: Oxford University Press, 2012) 178.
- <sup>91</sup> ECtHR, *Dupuis and others v. France* (App. No. 1914/02, 7 June 2007). [37].
- <sup>92</sup> *Guja* [74].
- <sup>93</sup> *Ibid.*
- <sup>94</sup> *Guja* at [87]
- <sup>95</sup> *Guja* at [88].
- <sup>96</sup> Latimer Paul and Brown A.J., ‘Whistleblower Laws: International Best Practice’ 31 *UNSW Law Journal* 31 (2008): 782.
- <sup>97</sup> Dirk Voorhoof, *The Right to Freedom of Expression and Information under the European Human Rights System : Towards a more transparent democratic society* (European University Institute, 2014) [http://cadmus.eui.eu/bitstream/handle/1814/29871/RSCAS\\_2014\\_12.pdf?sequence=1](http://cadmus.eui.eu/bitstream/handle/1814/29871/RSCAS_2014_12.pdf?sequence=1) pg 18.
- <sup>98</sup> ECtHR, *Voskuil v. Netherlands*. (App No. 64752/01, 22 November 2007).
- <sup>99</sup> *Heinisch* [66], *Dupuis* [40], ECtHR., *Surek v. Turkey (no. 1)* (App. No. 26682/95, 8 July 1999)[61].
- <sup>100</sup> *Dupuis* [41]. See also ECtHR, *Fressoz and Roire v. France* (App. No. 29183/95, 21 January 1999).
- <sup>101</sup> Cameron, *National Security*, 42.
- <sup>102</sup> *Bucur* [101].
- <sup>103</sup> Luban, ‘Taking out the adversary: The Assault on Progressive Public-Interest Lawyers’, *California Law Review* 91 (2003): 210.
- <sup>104</sup> See Hersh Marion, ‘Whistleblowers - Heroes or traitors? Individual and Collective Responsibility for Ethical Behaviour’, *Annual Reviews in Control* 26 (2002): 244 and Martin Brian, ‘Illusions of Whistleblower Protection’, *UTS Law Review* 5 (2003): 122.
- <sup>105</sup> In the Snowden case for instance, a federal judge held that the policy of the intelligence agencies that Snowden disclosed was lawful. See *ACLU v. Clapper* (No. 13-3994, S.D. New York 28 December 2013).
- <sup>106</sup> Popelier Patricia and Catherine Van De Heyning, ‘Procedural Rationality: Giving Teeth to the Proportionality Analysis’, *European Constitutional Law Review* 9 (2013): 238.
- <sup>107</sup> See Open Society Foundations, *The Global Principles on National Security and the Right to Information 2013* (Tshwane Principles) available at <http://www.opensocietyfoundations.org/sites/default/files/global-principles-national-security-10232013.pdf>. Principle 40 argues that “the “reasonably believed” test is a mixed objective-subjective test. The person must actually have held the belief (subjectively), and it must have been reasonable for him or her to have done so (objectively) ... [I]t is ultimately for an independent court or tribunal to determine whether this test has been satisfied so as to qualify the disclosure for protection”.
- <sup>108</sup> Transparency international, ‘Whistleblower Laws’, 7.
- <sup>109</sup> Lewis David, ‘Enterprise and regulatory reform – whistleblowing aspects’, *Employment Law Bulletin* 110 (2012): 5.
- <sup>110</sup> See note 74 above.
- <sup>111</sup> Banisar, “Whistleblowing: International Standards and Developments” at 2.
- <sup>112</sup> *Ibid* at 23.
- <sup>113</sup> *Ibid.* For a specific list of countries and an exhaustive state by state analysis see Banisar David, *Freedom of Information around the World: A Global Survey of Access to Government Information Laws* (Privacy International, 2006) available at [http://www.freedominfo.org/documents/global\\_survey2006.pdf](http://www.freedominfo.org/documents/global_survey2006.pdf) and Banisar ‘Whistleblowing International Standards’.
- <sup>114</sup> Latimer and Brown, ‘Whistleblower Laws’, 785.
- <sup>115</sup> However, the UN Rapporteur on Freedom of Opinion and Expression has attempted to define certain areas where disclosures ought to enjoy free speech protection. The 2000 report stated that: “Individuals should be protected ... for releasing information on wrongdoing, viz. the commission of a criminal offence or dishonesty, failure to comply with a legal obligation, a miscarriage of justice, corruption or dishonesty or serious failures in the administration of a public body”. UN Economic and Social Council- Commission on Human Rights 56<sup>th</sup> session. ‘Civil and Political Rights including the question of Freedom of Expression’ E/CN.4/2000/63 18 January 2000 [44].
- <sup>116</sup> Banisar, ‘Whistleblowing International Standards’, 25.
- <sup>117</sup> South African Protected Disclosures Act 2000, [http://www.justice.gov.za/legislation/notices/2011/20110831\\_gg34572\\_n702-disclosure-guidelines.pdf](http://www.justice.gov.za/legislation/notices/2011/20110831_gg34572_n702-disclosure-guidelines.pdf) pg 4
- <sup>118</sup> Banisar, ‘Whistleblowing International Standards’, 25
- <sup>119</sup> Callahan, Dworkin and Lewis, ‘Australia, U.K., and U.S. approaches to Disclosure in the Public Interest’, *Virginia Journal of International Law* 44 (2003-2004): 886.
- <sup>120</sup> 5 U.S.C. § 2302(b)(8)(A)(ii) (2003).

- 
- <sup>121</sup> Callahan, Dworkin and Lewis at 886 and 42 U.S.C. § 300j-9(i) (2002).
- <sup>122</sup> Banisar, ‘Whistleblowing International Standards’, 25.
- <sup>123</sup> Transparency International ‘Whistleblower Laws’, 10.
- <sup>124</sup> Tshwane Principles, Principle 37.
- <sup>125</sup> Resolution 1954 (2013) at [9.5].
- <sup>126</sup> Ibid.
- <sup>127</sup> Chelsea Manning’s disclosure of a video of US crew killing Iraqi civilians would fall under the protected category of a violation of International Humanitarian Law, Snowden’s disclosures would fall under mass surveillance, while NSA employee Thomas Drake’s revelations of waste of funds in the NSA would fall under waste of resources.
- <sup>128</sup> Tshwane Principles, Principle 10.
- <sup>129</sup> Ibid at D1.
- <sup>130</sup> Ibid.
- <sup>131</sup> An example of this would be David Kelly, an employee of the Defence Intelligence Staff in the UK, who leaked information to the press that refuted the official government line on the rationale behind the war in Iraq. After the disclosure Kelly committed suicide and an inquiry was established over the circumstances of his death. Lord Hutton, ‘Report of the Inquiry into the Circumstances Surrounding the Death of Dr David Kelly C.M.G.’, HC 247 2003/4.
- <sup>132</sup> Tshwane Principles, Principle 37.
- <sup>133</sup> Buckland Benjamin and Wills Aidan, ‘Whistleblowing in the Security Sector’ available at <http://whistlenetwork.files.wordpress.com/2014/01/bucklandwills-chapter.pdf>
- <sup>134</sup> Venice Commission Report, ‘Oversight of Security Services’, 18.
- <sup>135</sup> UK Prime Minister Report to Parliament, ‘A Strong Britain In an Age of Uncertainty: The National Security Strategy’, October 2010 (Cm7953) available at [https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/61936/national-security-strategy.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/61936/national-security-strategy.pdf) at 24.
- <sup>136</sup> French Labour Code Article L 1161-1 found in Guyer and Peterson ‘The Current State of Whistleblower Law in Europe: A Report by the Government Accountability Project’ 2013 American Bar Association Section Of Labor & Employment Law International Labor & Employment Law Committee <http://www.whistleblower.org/storage/documents/TheCurrentStateofWhistleblowerLawinEurope.pdf> pg15.
- <sup>137</sup> Papandrea Mary-Rose, ‘The Publication of National Security Information in the Digital Age’, *Journal of National Security Law and Policy* 5(2011-2012): 199. See also, Benkler Yochai, ‘A Free Irresponsible Press: Wikileaks and the Battle over the Soul of the Networked Fourth Estate’, *Harvard Civil Rights – Civil Liberties Law Review* 46 (2011): 311.
- <sup>138</sup> Martin Brian, *Justice Ignited: The Dynamics of Backfire* (Lanham, MD: Rowman & Littlefield, 2007) at 67.