Parliamentary Assembly
Assemblée parlementaire
https://pace.coe.int

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Doc. 13791
19 May 2015

Improving the protection of whistle-blowers

Report[1]
Committee on Legal Affairs and Human Rights
Rapporteur: Mr Pieter OMTZIGT, Netherlands, Group of the European People's Party

Summary

The Committee on Legal Affairs and Human Rights stresses the importance of whistle-blowing for promoting good governance, privacy, freedom of speech and the fight against corruption, including in the fields of national security and intelligence.

It welcomes the adoption, by the Committee of Ministers, of Recommendation CM/Rec(2014)7 calling on member States to create an appropriate normative, judicial and institutional framework for the protection of whistle-blowers.

In view of the disclosures concerning mass surveillance and intrusions of privacy carried out by the United States National Security Agency and other intelligence agencies, which affect communications of numerous persons who are not suspected of any wrongdoing, the committee considers that whistle-blower protection measures should cover all individuals who denounce wrongdoings which place fellow human beings at risk of violations of their rights protected under the European Convention on Human Rights, including persons working for national security or intelligence agencies.

Given the importance of whistle-blowing to ensure that legal limits placed on mass surveillance are respected and the international ramifications of whistle-blowing in the field of national security or intelligence, whistle-blowers (including employees of relevant government agencies or private contractors), whose disclosures are otherwise in line with Resolution 1729 (2010), Committee of Ministers Recommendation CM/Rec(2014)7 or the Tshwane Principles as supported by Resolution 1954 (2013), should be granted asylum in a member State of the Council of Europe when they are persecuted in their home country.

1. Reference to committee: Doc. 13278, Reference 3998 of 30 September 2013.

Contents **Page**

A. Draft resolution[2]

1. The Parliamentary Assembly recalls its Resolution 1729 (2010) and Recommendation 1916 (2010) on the protection of "whistle-blowers" inviting all Council of Europe member States to improve the protection of whistle-blowers, strengthen accountability and bolster the fight against corruption and mismanagement, both in the public and private sectors.

2. It further recalls its Resolution 1954 (2013) and Recommendation 2024 (2013) on national security and access to information, supporting the Tshwane Principles (The Global Principles on National Security and the Right to Information) to improve the balance between the public's right to know and the protection of legitimate national security concerns.

3. The Assembly stresses the importance of the case law of the European Court of Human Rights, upholding the right to privacy, freedom of speech and the protection of whistle-blowers, including in the fields of national security and intelligence.

4. It further welcomes the recent adoption, by the Committee of Ministers, of Recommendation CM/Rec(2014)7 calling on member States to create an appropriate normative, judicial and institutional framework for the protection of whistle-blowers.

5. It notes that the Council of Europe has set up guidelines for staff members on reporting wrongdoing; these guidelines, which establish internal reporting channels, reflect some, but not all, of the principles advocated by the Assembly and the Committee of Ministers.

6. In view of the disclosures concerning mass surveillance and intrusions of privacy carried out by the United States National Security Agency (NSA) and other intelligence agencies, which affect the communications of numerous people who are not suspected of any wrongdoing, the Assembly notes with regret that disclosures of information related to national security are generally excluded from protection available to whistle-blowers.

7. The Assembly considers that whistle-blower protection measures should cover all individuals who denounce wrongdoings which place fellow human beings at risk of violations of their rights protected under the European Convention on Human Rights (ETS No. 5), including people working for national security or intelligence agencies.

8. In view of the importance of whistle-blowing to ensure that legal limits placed on mass surveillance are respected (see Resolution 2045 (2015) on mass surveillance, paragraph 13), and in view of the international ramifications of whistle-blowing in the field of national security or intelligence, the Assembly considers that whistle-blowers (including employees of relevant government agencies or private contractors), whose disclosures are otherwise in line with Resolution 1729 (2010), Committee of Ministers Recommendation CM/Rec(2014)7 or the Tshwane Principles as supported by Resolution 1954 (2013), should be granted asylum in any member State of the Council of Europe when they are persecuted in their home country.

9. The Assembly therefore calls on:

9.1. Council of Europe member and observer States and the European Union, as applicable, to:

9.1.1. enact whistle-blower protection laws also covering employees of national security or intelligence services and of private firms working in this field;

9.1.2. grant asylum, as far as possible under national law, to whistle-blowers threatened by retaliation in their home countries, provided their disclosures qualify for protection under the principles advocated by the Assembly;

9.1.3. agree on a binding legal instrument (convention) on whistle-blower protection on the basis of Committee of Ministers Recommendation CM/Rec(2014)7, taking into account recent developments;

9.2. the United States of America to allow Mr Edward Snowden to return without fear of criminal prosecution under conditions that would not allow him to raise the public interest defence.

2. Draft resolution adopted by the committee on 18 March 2015.

B. Draft recommendation[3]

1. The Parliamentary Assembly recalls its Resolution … (2015) "Improving the protection of whistle-blowers" as well as its Recommendation 1916 (2010) on the protection of "whistle-blowers".

2. The Assembly welcomes the adoption by the Committee of Ministers of Recommendation CM/Rec(2014)7 on the protection of whistleblowers, as an important step in the right direction.

3. The Assembly invites the Committee of Ministers to:

3.1. promote further improvements for the protection of whistle-blowers by launching the process of negotiating a binding legal instrument in the form of a framework convention that would be open to non-member States and cover disclosures of wrongdoings by persons employed in the field of national security and intelligence;

3.2. meanwhile, consider ways and means to provide Council of Europe technical assistance to member States for the implementation of Recommendation CM/Rec(2014)7;

3.3. encourage the Secretary General to further improve the whistle-blowing rules applicable in the Council of Europe, with a view to bringing them fully into line with the principles upheld by the Assembly and the Committee of Ministers.

3. Draft recommendation adopted by the committee on 18 March 2015.

C. Explanatory memorandum by Mr Omtzigt, rapporteur

1. Introduction

1. From bribery to corruption, fraud to human rights violations, whistle-blowers have helped us in the fight against impunity by disclosing wrongdoings in both the public and private sector. Protecting individuals who contribute to public debate by disclosing information helps improve democratic accountability, governance and the protection of human rights. The Parliamentary Assembly has previously encouraged States to develop legal frameworks and implement proper channels to receive and follow up disclosures by whistle-blowers, strengthen protection against retaliation for individuals who make public interest disclosures and foster an environment where individuals feel less threatened when disclosing wrongdoings.[4]

2. The disclosures made by Edward Snowden have once again demonstrated the importance of whistle-blowing, by shedding light on abuses by the intelligence sector, which has so far been *de facto* excluded from whistle-blower protection measures. The documents leaked with the help of Mr Snowden have revealed that States can intercept communications and access personal data in virtually any form, from anyone, at any time and in any place. The revelations have sparked a global debate on the use of technology affecting people's privacy, a practice many had worried about but were unable to denounce, due to lack of evidence, in view of the pervasive secrecy surrounding the activities of intelligence agencies.

3. On 6 November 2013, the Committee on Legal Affairs and Human Rights appointed me as rapporteur for two interrelated subjects, namely: "Massive eavesdropping"[5] and "Additional Protocol to the European Convention on Human Rights on Protection of whistle-blowers".[6] After a first round of discussions on 6 November 2013, the committee decided, at its meeting on 27 January 2014, on the basis of my introductory memorandum,[7] to change the title of the future report from "Additional Protocol to the European Convention on Human Rights on the protection of whistle-blowers" to "Improving the protection of whistle-blowers", and to invite Mr Snowden and Ms Anna Myers, co-ordinator of the "Whistleblowing International Network" (WIN), to an exchange of views with the committee. Unfortunately, as for the hearing on "Mass Surveillance" in April 2014, it was not possible to receive the necessary assurances which would have allowed Mr Snowden to come safely to Strasbourg and to freely travel to a country of his choosing after the hearing. The committee therefore had to content itself with hearing Mr Snowden, during its meeting on 24 June 2014, via a live video link from his temporary place of asylum in Moscow.[8] I should like to thank Mr Snowden for his readiness to address the committee and to answer questions "live", despite possible legal risks. I have described the disclosures and their consequences in some detail in the report on "Mass surveillance", which the committee adopted unanimously at its meeting on 26 January 2015.[9] On 29 January 2015, the committee also had an exchange of views with Ms Maria Bamieh, a British prosecutor with the European Union Rule of Law Mission in Kosovo*[10] (EULEX), who had blown the whistle on alleged corruption within EULEX itself, and heard a statement from prison by Central Intelligence Agency (CIA) whistle-blower John Kiriakou, presented via live video link by his lawyer, Jesselyn Radack, herself a whistle-blower who had worked in the United States Department of Justice.

4. More so than in other whistle-blowing cases, different and sometimes contradictory interests come to bear when disclosures involve national intelligence information. The whistle-blower's freedom of expression and the people's freedom of information clashes with the intelligence agent's duty to protect secret information; transparency and democratic accountability clash with the need for secrecy for intelligence operations to be effective. Yet, the legitimate need for secrecy and confidentiality should not be abused as a cloak to conceal human rights violations committed by government agents. Even after legal limits are placed on surveillance and reasonably effective parliamentary or judicial oversight mechanisms are set up to ensure that intelligence agencies are accountable to the public, which is not yet the case in most countries, whistle-blowing – the "sword of Damocles" of protected disclosures of violations – is an important tool for ensuring that legal limits for surveillance are in fact respected.

---

4. See Resolution 1729 (2010) and Recommendation 1916 (2010).
5. Motion for a resolution, Doc. 13288.
6. Motion for a recommendation, Doc. 13278.
7. Document AS/Jur (2014) 2, 23 January 2014.
8. [Video testimony of Edward Snowden on 26 June 2014.]
9. Document AS/Jur (2015) 1, 19 January 2015.
10. * All reference to Kosovo, whether to the territory, institutions or population, in this text shall be understood in full compliance with United Nations Security Council Resolution 1244 and without prejudice to the status of Kosovo.

5. As pointed out in my previous report on whistle-blower protection, adopted by the Assembly in January 2010, most member States of the Council of Europe had at that time no effective legislative framework for protecting bona fide whistle-blowers who disclose serious violations of human rights or corruption, let alone a generally accepted statutory definition of who qualifies as a "whistle-blower". Many countries still lacked awareness of the very concept of "whistle-blowing", not to be confounded with notions such as "snitching", which have a strong pejorative undertone especially in countries that have endured periods of totalitarian or authoritarian rule; nor should the solution be seen only with respect to strengthening "witness protection", which necessarily involves the criminal justice system.

6. A certain amount of progress can be observed since 2010, for which the Assembly's earlier resolution surely deserves some credit. According to a study published by Transparency International in 2013 limited to the member States of the European Union, four EU countries (Luxembourg, Romania, Slovenia, and the United Kingdom) had legal frameworks for whistle-blower protection deemed "advanced", while of the other 23 EU States,[11] 16 had partial legal protection for employees who report wrongdoings and the remaining seven had very limited or no legal frameworks.[12] However, even of those legal frameworks deemed "advanced", not all such laws cover individuals working in both the public and private sectors.

7. The "G20 Compendium of Best Practices and Guiding Principles for Legislation on the Protection of Whistleblowers"[13] prepared by the Organisation for Economic Co-operation and Development (OECD) and "supported" by the G20 at its summit in Cannes in November 2011 as part of the G20 anti-corruption action plan, advocates six guiding principles for the creation and review of a legal framework for whistle-blower protection. States must ensure that the legislation:

– puts in place a clear and effective institutional framework to protect employees from any disciplinary action or other forms of discrimination when they disclose in good faith and on reasonable grounds certain suspected acts of wrongdoing or corruption to competent authorities;

– lays down a clear definition of the scope of protected disclosures and of the persons afforded protection under the law;

– ensures that the protection afforded to whistle-blowers is robust and comprehensive;

– clearly defines the procedures and prescribed channels for facilitating the reporting of suspected acts of corruption, and encourages the use of protective and easily accessible whistle-blowing channels;

– ensures that effective protection mechanisms are in place, including by entrusting a specific body that is accountable and empowered to receive and investigate complaints of retaliation and/or improper investigation, and by providing a full range of remedies;

– that the implementation of whistle-blower protection legislation is supported by awareness-raising, communication, training and periodic evaluation of the effectiveness of the framework of protection.

8. The present report will first examine the Council of Europe's acquis in the field of whistle-blower protection, including previous work of the Assembly, the case law of the European Court of Human Rights ("the Court"), and the recent recommendation of the Committee of Ministers. In presenting the Committee of Ministers recommendation, I will suggest some additional measures States should consider in light of recent developments to improve the protection of whistle-blowers, regardless of the sector of activity in which they work or the public or private status of their employers. Before drawing some conclusions, I will take a closer look at the situation of whistle-blowers who work in the national security sector, with special attention given to the case of Edward Snowden.

2. The Council of Europe's acquis: promoting human rights and encouraging public debate through whistle-blower protection

2.1. The Parliamentary Assembly's previous work

9. The Council of Europe has consistently and continuously welcomed contributions by whistle-blowers to public debates on human rights issues when their disclosures were the last resort to fight impunity for corruption and other serious human rights violations.

---

11. Croatia, which joined the EU in July 2013, was not yet included in this overview.
12. Transparency International, Whistleblowing in Europe: Legal Protections for Whistleblowers in the EU (2013).
13. G20 Study: Whistleblower Protection Frameworks, Compendium of Best Practices and Guiding Principles for Legislation.

10. My previous report on the "Protection of whistle-blowers" (Resolution 1729 (2010) and Recommendation 1916 (2010)) helped establish the groundwork. The Assembly recognised whistle-blowing as a way of stopping wrongdoing that places people at risk, an opportunity to strengthen accountability and a tool to bolster the fight against corruption and mismanagement in both the public and private sectors. The resolution explicitly stated that whistle-blower legislation should cover members of the armed forces and special services. The review of the meagre whistle-blower protection at that time in different States led to the conclusion that substantial efforts were warranted in creating, improving, and enforcing whistle-blower protection, with certain guiding principles for States to bear in mind.

11. The Assembly recommended *inter alia* that:

– legislation should provide effective protection for bona fide whistle-blowers, who use existing internal whistle-blowing channels, from any form of retaliation;

– where internal channels either do not exist or do not function properly or could not reasonably be expected to do so, external whistle-blowing (including through the media) should likewise be protected;

– any whistle-blower should be considered as acting in good faith, as long as he or she had reasonable grounds to believe that the information disclosed was true, even if it later turns out that this was not the case, and he or she had no unlawful or unethical ulterior motive;

– States should ensure that a proper enforcement mechanism exists to investigate the disclosures and seek corrective action;

– the Council of Europe should set a good example by establishing its own whistle-blowing mechanism within the Organisation.

12. The Assembly subsequently adopted several other resolutions and recommendations referring to whistle-blowing as an effective means of enhancing, *inter alia*, government transparency, the respect for human rights and good governance.

13. In Resolution 1838 (2011) "Abuse of State secrecy and national security: obstacles to parliamentary and judicial scrutiny of human rights violations" (rapporteur: Mr Dick Marty, Switzerland, ALDE), the Assembly affirmed the need for proper judicial and parliamentary scrutiny of a government and its agents in order to maintain the rule of law and democracy, especially for secret services. The Assembly pointed out that information concerning the responsibility of State agents who have committed serious human rights violations (for example murder, enforced disappearance, torture, abduction) should not be protected as legitimate State secrets. The report examined in some detail the different judicial and parliamentary investigations carried out by Council of Europe member States following the disclosures of serious human rights violations committed by the CIA in collusion with the services of several European States in earlier reports of the Parliamentary Assembly on CIA secret prisons and "renditions".[14] The Assembly noted the non-existence or gross inadequacy of many member States' parliamentary or judicial supervision of their security and intelligence services. It therefore called for adequate protection for journalists and their sources[15] and for whistle-blowers,[16] as an additional method of oversight to help detect and deter human rights violations committed by members of secret services.

14. In Resolution 1954 (2013) on national security and access to information (rapporteur: Mr Arcadio Díaz Tejera, Spain, SOC), the Assembly emphasised the need for robust oversight over the activities of secret services, the protection of bona fide disclosures of wrongdoings by "whistle-blowers" and the availability of a "public interest override" as a safeguard against overly broad "national security" exceptions from the general rule of free accessibility of all information held by public authorities. This report addressed problems arising from information showing that State agents had committed serious human rights violations such as murder, enforced disappearance, torture or abduction, but were shielded from accountability because their actions were considered as "State secrets". The Assembly expressed its support for the "Global Principles on National Security and the Right to Information" (also known as the "Tshwane Principles"),[17] which include useful language on whistle-blower protection in the context of national security, and in particular the need for a

---

14. See "Alleged secret detentions and unlawful inter-State transfers of detainees involving Council of Europe member States", Doc. 10957, Resolution 1507 (2006) and Recommendation 1754 (2006), and "Secret detentions and illegal transfers of detainees involving Council of Europe member States: second report", Doc. 11302, Resolution 1562 (2007) and Recommendation 1801 (2007) (rapporteur for both: Dick Marty, Switzerland, ALDE).
15. Recommendation 1950 (2011) on the protection of journalist sources.
16. Resolution 1729 and Recommendation 1916 (2010) on the protection of "whistle-blowers".
17. www.opensocietyfoundations.org/publications/global-principles-national-security-and-freedom-information-tshwane-principles.

strong public interest defence. The "Tshwane Principles", which were endorsed by the Assembly in 2013, had in turn picked up the Assembly's earlier statement from the 2011 report by Dick Marty (Resolution 1838 (2011), see above), which asserts that information concerning the responsibility of State agents who have committed human rights violations should not enjoy protection as a legitimate State secret.

2.2. The case law of the European Court of Human Rights

15. The European Court of Human Rights has also developed principles for protecting freedom of expression in the context of whistle-blower cases, including cases concerning civil servants and even employees of a national intelligence service. New applications brought before the Court against mass surveillance programmes that were disclosed through the Snowden files are still pending,[18] but earlier judgments provide good starting points to distil key principles on how to balance freedom of expression and information, especially when denouncing misconduct, including unlawful actions and human rights violations, and the duty to maintain national security-related information secret.

16. Article 10 of the European Convention on Human Rights protects freedom of expression, which includes the "freedom to receive and impart information and ideas without interference by public authority". In its second paragraph, Article 10 subjects the exercise of these freedoms "to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary".

17. In *Guja v. Moldova*,[19] the European Court of Human Rights applied a balancing test to assess whether the State's interference with the freedom of expression of the applicant (a whistle-blower) was in accordance with Article 10.2 of the European Convention on Human Rights and ultimately found a violation. In this case, the applicant sent two letters that were not marked as confidential to the *Jurnal de Chişinău*, which published the communications to show that public officials were putting pressure on law-enforcement bodies. One letter was a note written by the Deputy Speaker of Parliament, Mr Mişin, to the Prosecutor General's Office and the second by the Deputy Minister in the Ministry of Interior, Mr A. Uraschi, to a Deputy Prosecutor General in order to exert pressure concerning the handling by the prosecution of criminal proceedings against four police officers, one of whom was accused of, *inter alia*, ill-treatment and unlawful detention. The applicant and another prosecutor who was suspected of having furnished the letters to the applicant were dismissed, with the dismissal notice stating that the letters disclosed to the newspaper were secret and that he had failed to consult his superiors prior to disclosing them.

18. The Court found a violation of Article 10. It first determined that "Article 10 was applicable in the present case, irrespective of the fact that he [the applicant] was not the author of the articles that had been sent to the newspaper" since "the protection of Article 10 extends to the workplace in general and to public servants in particular" as previously stated in cases against Germany, Liechtenstein, the United Kingdom and Spain.[20] Although it acknowledged the existence of the civil servants' duty of loyalty, reserve and discretion to their employer, the Court found that:

> *"the signalling by a civil servant or an employee in the public sector of illegal conduct or wrongdoing in the workplace should, in certain circumstances, enjoy protection. This may be called for where the employee or civil servant concerned is the only person, or part of a small category of persons, aware of what is happening at work and is thus best placed to act in the public interest by alerting the employer or the public at large".*[21]

19. The Court thus endorsed the position that disclosures in the public domain should serve as a last resort, once the civil servant has consulted a "superior or other competent authority or body. It is only where this is clearly impracticable that the information could, as a last resort, be disclosed to the public".[22]

---

18. See pending case of *Big Brother Watch and Others v. United Kingdom*, Application No. 58170/13, case communicated on 7 January 2014, and other cases to the European Court of Human Rights in *MTI-EcoNews*/Hungary, 29 November 2013, "NGO to turn to Strasbourg court over security services' secret surveillance".
19. Application No. 14277/04, judgment of 12 February 2008.
20. *Vogt v. Germany* (Application No. 17851/91, judgment of 2 September 1995, paragraph 53), *Wille v. Liechtenstein* (Application No. 28396/95, judgment of 28 October 1999, paragraph 41), *Babar Ahmed and Others v. the United Kingdom* (Applications Nos. 24027/07, 11949/08, 36742/08, 66911/09 and 67354/09, judgment of 2 September 1998, paragraph 56, and *Fuentes Bobo v. Spain* (Application No. 39293/98, judgment of 29 February 2000, paragraph 38).
21. *Guja v. Moldova*, op. cit., paragraph 72.
22. Ibid., paragraph 73.

20. Using a balancing test that incorporates different factors, the Court reached the conclusion that the government's interference with the applicant's freedom of expression was not proportionate to the interests sought to be protected by the government. First, it assessed whether the applicant had alternative channels for the disclosure, which he did not since there was no legislation or internal regulation in the Republic of Moldova for reporting irregularities by employees. Second, it assessed the nature of the public interest at stake with the disclosed information, which the Court found to weigh in the applicant's favour, since the practice of interference by politicians with criminal justice was a widely covered subject that the President of the Republic of Moldova himself had campaigned against in order to strengthen judicial independence. As it made this conclusion, the Court also noted that "[t]he interest which the public may have in particular information can sometimes be so strong as to override even a legally imposed duty of confidence".[23]

21. Third, the Court assessed the authenticity of the disclosed information, which was established. Fourth, it balanced the damages, if any, suffered by the public authority as a result of the disclosure and whether they outweighed the interests promoted by the disclosure. Although the letters to the Prosecutor General's Office were found to have had strong negative effects on public confidence in the independence of the institution, the Court considered the public interest of having information about undue pressure and wrongdoing on the judiciary to be extremely important in a democratic society, since "open discussion of topics of public concern is essential to democracy, and regard must be had to the great importance of not discouraging members of the public from voicing their opinions on such matters".[24]

22. Fifth, the Court assessed the applicant's motivations for the disclosure and noted that he had acted in good faith. Sixth and last, the Court weighed the severity of the sanction against other factors, concluding that applying the heaviest sanction possible on the applicant would seriously discourage other employees from reporting any misconduct.

23. Similarly in *Heinisch v. Germany*,[25] the European Court of Human Rights affirmed that "the public interest in being informed about the quality of public services outweighs the interests of protecting the reputation of any organisation".

24. Ms Heinisch became a whistle-blower when she disclosed information about the alleged deficiencies in the care provided by the public health institution where she worked as a nurse. Her employment contract was subsequently terminated, which the Court found was an interference with the applicant's freedom of expression guaranteed under Article 10. The clause's second section defines cases in which the State may interfere with an individual's exercise of freedom of expression: first, the restrictions or conditions must be "prescribed by law", and second, they must be "necessary in a democratic society" for the reasons listed in the provision. The Court found in the Heinisch case that while the termination of an employment relationship without notice was indeed "prescribed by law", the information that the applicant disclosed in good faith was "undeniably of public interest"[26] and of seeming authenticity. The Court found that she had made sufficient internal complaints prior to making a criminal complaint. The Court's position reflects the Council of Europe's longstanding support for transparency, freedom of expression and information, government accountability and the fight against corruption.

25. In *Sosinowska v. Poland*,[27] another case concerning the health sector,[28] the applicant, a specialist working in a hospital, was dismissed from her job for "expressing negative opinions about the head physician's qualifications", thereby breaching the "principle of professional solidarity". The Court found that the applicant was "penalised essentially for the fact that she had expressed concerns, to persons working in the ward, to the hospital's authorities and to the regional consultant, about the quality of the medical care given to patients on her superior's orders". The applicant's comments concerned issues of "public interest"[29] and were therefore covered by her freedom of speech guaranteed by Article 10 and should not have given rise to disciplinary sanctions.

---

23. Ibid., paragraph 74.
24. Ibid., paragraph 91.
25. Application No. 28274/08, judgment of 21 July 2011.
26. Ibid., paragraph 71.
27. Application No. 10427/09, judgment of 18 October 2011.
28. In the health sector, whistle-blowing plays an especially important role to defend patients' rights in the face of powerful structures. The UK National Health Service (NHS) has benefited from important reforms triggered by whistle-blowers drawing attention to serious shortcomings. Nevertheless, a Government-commissioned inquiry led by Sir Robert Francis QC recently documented "shocking" accounts of the treatment of whistle-blowers by the NHS (see *The Guardian*, 11 February 2015, "NHS whistle-blowers ignored, bullied and intimidated, inquiry finds"; see also the statement by Public Concern At Work of 11 February 2015.
29. Ibid., paragraphs 79 and 83.

26. In *Bucur and Toma v. Romania,*[30] the first applicant, who worked for the Romanian Intelligence Service, disclosed by way of holding a press conference that the this service had unlawfully tapped the phones of a large number of journalists, politicians and businessmen. An opposition member of the parliamentary committee tasked with supervising the Romanian Intelligence Service, whom the applicant had first contacted, advised him to go public straightaway because the committee, dominated by the ruling party, would not take any action anyway. The applicant was found guilty of the crime of breach of official secrecy. The European Court of Human Rights found that the conviction breached the applicant's right to freedom of expression (Article 10 of the European Convention on Human Rights) as the prosecution was not "necessary in a democratic society". The Court stressed the fact that at the time of the disclosure, the new laws providing a legal framework for whistle-blowing had not yet been adopted and that the applicant had no other effective means of imparting the information on the abuses. It also stressed the high public interest value of the information imparted, which related to abuses committed by high-ranking officials and affected the democratic foundations of the State. The Court also found a violation of the other applicants' (who were victims of the unlawful surveillance) privacy rights (Article 8 of the Convention).

27. The latest in the series of judgments strengthening the protection of whistle-blowers is the case of *Matúz v. Hungary.*[31] The Court unanimously found a violation of Article 10 after the Hungarian courts upheld the dismissal of a whistle-blowing journalist employed by the Hungarian State television company. The applicant had, in breach of the confidentiality clause in his employment contract, published a book criticising his employer for alleged censorship by a director of the company.

28. The Court found that the dismissal was prompted only by the publication of his book, without taking into account the journalist's professional ability, and thus constituted an interference with the exercise of his freedom of expression. That interference had not been "necessary in a democratic society", because the applicant's conduct had been in the public interest, namely to draw public attention to censorship within the State television. The Court took into account that the applicant had acted in good faith, and the book was published only after the applicant had unsuccessfully tried to complain about the alleged censorship to his employer. It also noted that the domestic courts had found against the applicant solely on the ground that publication of the book breached his contractual obligations, without considering his argument that he was exercising his freedom of expression in the public interest.

2.3. Committee of Ministers Recommendation CM/Rec(2014)7

29. In response to the Assembly's 2010 report on the protection of whistle-blowers, the Committee of Ministers issued Recommendation CM/Rec(2014)7 on the protection of whistleblowers. The recommendation largely reflects the Assembly's position expressed in Resolution 1729 (20 10) and Recommendation 1916 (2010). The Committee of Ministers recognised, in particular, the need for States to enact comprehensive whistle-blower legislation to encourage and protect bona fide warnings against various violations of the law, including violations of human rights. It rightly advised States to adopt a "comprehensive and coherent approach to facilitating public interest reporting and disclosures".[32] Multiple provisions scattered over different areas of law may prevent potential whistle-blowers from having a clear understanding of the legal provisions that apply in particular cases.

2.3.1. Personal and material scope

30. In recommending States to enact legislation that provides a clear definition of the scope of protected disclosures and of the persons afforded protection under the law, the Committee of Ministers' recommendation is more thorough than the Assembly's resolution in defining the personal scope of whistle-blower protection. It covers individuals who already have a "work-based relationship", as well as those who have acquired information concerning a threat or harm to the public interest "during the recruitment process or other pre-contractual negotiation stage" (paragraphs 3-4).

31. Nevertheless, the Committee of Ministers has carved out too wide an exception for the intelligence sector. Paragraph 5 of the Committee of Ministers recommendation allows for "special schemes or rules, including modified rights and obligations" to apply for information "relating to national security, defence, intelligence, public order or international relations of the State". But nowhere in the recommendation is "national security" defined. In light of the Snowden disclosures, a more specific framework for national

30. Application No. 40238/02, judgment of 8 January 2013.
31. Application No. 73571/10, judgment of 21 October 2014.
32. Appendix to Recommendation CM/Rec(2014)7, paragraph 7.

security-related disclosures should be elaborated. Safeguards are needed in order to avoid intelligence agencies covering up serious human rights violations by improperly classifying all related information as matters of "national security".

32. In view of the "Tshwane Principles" supported by the Assembly in its Resolution 1954 (2013),[33] States should clearly define in their laws the narrow categories of information that may be withheld on national security grounds (Principle 3.*c*). Tshwane Principle 37 lists categories of wrongdoings that are typically of high interest to the public and that public servants should be allowed to disclose without fear of retaliation. Wrongdoings that qualify for "protected disclosures", include criminal offences, violations of human rights and international humanitarian law, corruption, dangers to public health and safety, dangers to the environment, abuse of public office, miscarriages of justice, mismanagement or waste of resources, retaliation for disclosing any of the mentioned categories of wrongdoing, and deliberate concealment of any matter falling into one of the mentioned categories.

33. Tshwane Principle 10 lists several categories of information that are of especially high public interest and that should therefore even be published proactively and never withheld. They include information relating to gross violations of international human rights and humanitarian law, systematic and widespread violations of the rights to personal liberty and security and other ill-treatment. Notably, Principle 10.E.1 specifies that "[t]he overall legal framework concerning surveillance of all kinds, as well as the procedures to be followed for authorizing surveillance, selecting targets of surveillance, and using, sharing, storing, and destroying intercepted material, should be accessible to the public".

34. Most importantly, the Tshwane Principles (Principle 43) require the availability of a "public interest defence" for public personnel, even when public personnel is subject to criminal or civil proceedings relating to their having made a disclosure not otherwise protected under these Principles, if the public interest in the disclosure of the information in question outweighs the public interest in non-disclosure.

35. States should therefore not make blanket rules or exceptions based merely on the sector of activity to which the whistle-blower belongs. Employees of intelligence agencies or relevant private contractors, just like other government or private sector employees, may come across serious wrongdoings in a work-related context. The sensitivity of the information and potential harm caused by the disclosure should be taken into account when deciding whether the public interest in disclosure outweighs the risk of harm, but the confidential nature of the information as such should not preclude a protected disclosure from the outset. Otherwise, governments could avoid any form of public scrutiny by overclassifying information.

2.3.2. Channels for and responses given to reports and disclosures

36. The Committee of Ministers incorporated the Assembly's main suggestions as to proper channels through which whistle-blowers can report and disclose information of unlawful acts, both in the public and private sectors. The Committee of Ministers listed different channels that whistle-blowers can use, including reports within an organisation or enterprise, reports to relevant public regulatory bodies, law-enforcement and supervisory bodies, and disclosures to the public. An additional contribution that the Committee of Ministers included in its recommendation was that whistle-blowers be "informed, by the person to whom the report was made, of the action taken in response to the report". It is well-known that whistle-blowers are primarily motivated by their desire to see misbehaviour stopped. Internal reporting channels are of no use if no effective investigation is made and no appropriate response is given to address the alleged misconduct. This provision therefore deserves to be especially welcomed.

37. But there is room for improvement. First, individuals or bodies processing such reports should be truly independent and empowered to act on the information provided by whistle-blowers. As explained in Tshwane Principle 39, oversight bodies should be "institutionally and operationally independent from the security sector and other authorities from which disclosures may be made, including the executive branch". It would be of no benefit to have internal reporting channels if their role was to simply dissuade potential whistle-blowers from coming forward. On the contrary, boards under the authority of the body implicated by accusations of wrongdoing would use this internal process to identify and persecute whistle-blowers before they even have a chance to report wrongdoing in an effective way.

38. Second, these bodies should have the actual ability to respond to and act upon whistle-blowers' reports. States should hence consider incorporating Tshwane Principle 39.B.3, which stipulates that "[t]he law should guarantee that independent oversight bodies have access to all relevant information and afford them the necessary investigatory powers to ensure this access. Such powers should include subpoena powers and

33. See paragraph 14 above.

the power to require that testimony is given under oath or affirmation". This Principle aptly translates the goals of paragraphs 19 and 20 of the Committee of Ministers' recommendation that reports by whistle-blowers reports should be promptly investigated and the whistle-blower informed about the progress made.

2.3.3. Confidentiality

39. The Committee of Ministers' recommendation, in paragraph 18, correctly reflects the Assembly's suggestion regarding the need to protect the identity of the whistle-blower, unless he or she consents to disclosure or disclosure is needed in order to avert imminent or serious threats to the public interest.

2.3.4. Protection from retaliation

40. Protecting whistle-blowers from retaliation not only encourages more individuals to come forward with information on serious human rights violations and other misconduct, but also protects their right to an effective remedy as provided by Article 13 of the European Convention on Human Rights. This article provides that "[e]veryone whose rights and freedoms as set forth in this Convention are violated shall have an effective remedy before a national authority notwithstanding that the violation has been committed by persons acting in an official capacity".

41. Protection against retaliation for making disclosures of information showing wrongdoing is also recommended in the Tshwane Principles (Principle 41). This includes protection from criminal as well as civil proceedings for the disclosure of classified or otherwise confidential information.

42. Overall, the Committee of Ministers followed the Assembly's suggestions for the defence of whistle-blowers against retaliation. The Committee of Ministers recommendation lists different forms of retaliation, such as "dismissal, suspension, demotion, loss of promotion opportunities, punitive transfers and reductions in or deductions of wages, harassment or other punitive or discriminatory treatment", which is broad enough to cover all types of possible retaliation.

43. I also support the Committee of Ministers' recommendations in paragraphs 11 and 22. Paragraph 11 establishes that "[a]n employer should not be able to rely on a person's legal or contractual obligations in order to prevent that person from making a public interest report or disclosure or to penalise him or her for having done so".

44. Paragraph 22 postulates that whistle-blower protection should not be lost "solely on the basis that the individual making the report or disclosure was mistaken as to its import or that the perceived threat to the public interest has not materialised, provided he or she had reasonable grounds to believe in its accuracy".

45. Such a position is in accordance with the Tshwane Principles, which guarantee protection from retaliation for a whistle-blower who had "reasonable grounds to believe that the information disclosed tends to show wrongdoing" that falls within one of the protected disclosures listed in Principle 37 and follows the proper (internal or external) reporting process.

46. The Committee of Ministers did not recommend that States create a downside risk for those committing acts of retaliation by exposing them to counter-claims from the victimised whistle-blower. I consider that such a downside risk could be effective in discouraging retaliatory actions.

47. In line with Tshwane Principle 41.D, the Committee of Ministers recommended that the employer shall bear the burden of proof as to whether a detriment suffered by the whistle-blower after the disclosure was motivated by retaliation, but it did not specify what level of proof is requisite for doing so. Paragraph 6.3 of Assembly Resolution 1729 (2010) is more specific in calling for the employer to be required to show "beyond reasonable doubt" that any measures taken to the detriment of a whistle-blower were motivated by reasons other than the action of whistle-blowing, in other words unrelated to the disclosure.

48. The Committee of Ministers' recommendation should in my view have been more specific about the circumstances in which whistle-blowers can resort to external disclosures to report wrongdoing and about the level of protection they have when doing so. While the Committee of Ministers calls for measures to implement internal reporting channels and measures to protect whistle-blowers, it does not specify when and under which conditions a whistle-blower can forego internal channels and proceed with external avenues, by disclosing information for instance to the media. The recommendation mentions in paragraph 24 that "[w]here an employer has put in place an internal reporting system, and the whistle-blower has made a disclosure to the public without resorting to the system, this may be taken into consideration when deciding on the remedies or level of protection to afford to the whistle-blower".

49. But what if the whistle-blower could not reasonably be expected to resort to those internal channels because they were not functional or because they could not reasonably be expected to be a viable option for the whistle-blower for other reasons, for example because previous whistle-blowers who resorted to these channels suffered from retaliation or did not manage to get their concerns properly addressed?

50. In paragraph 23, the Committee of Ministers recommendation advises that "whistle-blowers should be entitled to raise, in appropriate civil, criminal or administrative proceedings, the fact that the report or disclosure was made in accordance with the national framework".

51. This assumes and relies on the fact that the country concerned actually has a national framework for whistle-blowing in place. In addition, as mentioned before, the recommendation does not specify when States should deem it proper for whistle-blowers to resort to external channels. In fact, it only mentions in paragraph 17 that "[a]s a general rule, internal reporting and reporting to relevant public regulatory bodies, law enforcement agencies and supervisory bodies should be encouraged", leaving out external reporting channels. We can, however, foresee cases in which an internal reporting framework cannot be expected to work, because the body mandated to receive such reports lacks independence or includes individuals who may be in a conflict of interest situation.

52. I would refer to the Tshwane Principles for guidance on strengthening the legal framework for the (still exceptional) protection of public disclosures. The law should clearly define the conditions under which such protection is granted.

53. Principle 40 holds that the law should protect disclosures to the public if they meet certain conditions, namely one or more of four alternative criteria: previous unsuccessful internal disclosure; risk of concealment of the wrongdoing in case of an internal disclosure; non-existence of an internal disclosure mechanism; or imminent risk to life, health or safety of persons which can only be avoided by immediate external disclosure. In addition, there are two cumulative conditions, namely that the person making the disclosure only disclosed the amount of information that was reasonably necessary to bring to light the wrongdoing, and 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.

54. Especially since solid legal frameworks are not yet in place for whistle-blower protection in many Council of Europe member States, and since we have yet to see whether internal reporting mechanisms or oversight boards that have been or will be implemented are truly independent, a clear definition of the exceptional conditions under which whistle-blowers can resort to public channels seems essential in enhancing whistle-blower protection measures.

55. Finally, I would like to reiterate the point made by our expert, Ms Myers, at the hearing before the committee in June 2014.[34] Instead of debating whether any one individual whistle-blower is a traitor or a saint, the focus should be on whether the information delivered was properly assessed and investigated by those who received it, and whether those responsible for any harm or damage caused were properly held to account. In order to do so, it is primordial for States to ensure the existence of truly independent oversight bodies that receive and investigate protected disclosures and follow up whistle-blowers' reports in an appropriate manner while ensuring their protection.

2.3.5. Advice, awareness and assessment

56. I welcome two points included in the Committee of Ministers' recommendation in addition to the proposals the Assembly conveyed through Resolution 1729 (2010). First, paragraph 28 of the Committee of Ministers' recommendation calls for "making access to information and confidential advice free of charge for individuals contemplating making a public interest report or disclosure".

57. In addition, I fully support the suggestion that national authorities undertake periodic assessments of the effectiveness of their respective national framework for whistle-blower protection (paragraph 29 of the Committee of Ministers' recommendation). States can clearly benefit from such assessments, which should take into account existing guidelines and best practices, such as the G20 Compendium of Best Practices and Guiding principles for Legislation on the Protection of Whistleblowers and the Tshwane Principles.

---

34. Statement by Anna Myers, Lawyer and Expert Coordinator at Whistleblowing International Network, at the hearing on Strengthening the Protection of Whistle-blowers, organised by the Committee on Legal Affairs and Human Rights, 24 June 2014.

58. Finally, I also agree with the Committee of Ministers' recommendation (in paragraph 27) that national frameworks for whistle-blower protection be "promoted widely in order to develop positive attitudes amongst the public and professions and to facilitate the disclosure of information in cases where the public interest is at stake". As mentioned in paragraph 8 of Assembly Resolution 1729 (2010), non-governmental organisations (NGOs) can play a useful complementary role in fostering an environment that encourages open reporting or disclosure.

3. The Snowden disclosures: reassessing existing whistle-blower protection measures for the intelligence community

59. In light of new developments, in particular the disclosures by Edward Snowden that unveiled far-reaching mass surveillance programmes and interference with Internet security measures, we need to reassess existing whistle-blower protection measures with a view to proposing improvements as needed. The disclosure of national security-related information has been generally excluded from existing whistle-blower protection measures, even though such disclosures may well be necessary in order to uncover and deter abuses by secret services and hold their perpetrators to account.

60. The files leaked by journalists with the help of Mr Snowden have unquestionably contributed to the public interest by disclosing the nature and extent of mass surveillance taking place around the world and the threats to Internet security resulting from certain practices. In the related report on "Mass surveillance",[35] I summed up key disclosures describing the sophisticated techniques the United States National Security Agency (NSA) and other secret services have at their disposal, and make use of on a stunning scale, to intercept, analyse and store communications from unsuspecting and unsuspected individuals on all continents.

61. Were it not for Mr Snowden's contribution, we would still not know about the different programmes that intelligence agencies use on a daily basis, and which interfere with our privacy. Mr Snowden's disclosures enabled us to discover that the NSA could record every single phone call in an entire country,[36] access personal data held by leading Internet companies with or without their consent,[37] tap the phones of German Chancellor Merkel along with those of 121 other heads of State and government, and even spy on the United Nations, the European Union and other international organisations.[38] Some of these programmes were carried out in collaboration with, and others targeted allied States.

62. While intelligence agencies require confidentiality for their legitimate activities to function, such secrecy should clearly not be invoked to cover up abuses of power and provide impunity for unlawful behaviour that infringes the right to privacy and other human rights, under the radar of existing parliamentary and judicial oversight mechanisms whose functioning is notoriously hampered by the difficulty of access to information defined as secret by those who do not wish to disclose it. In order to deter and sanction transgressions, whistle-blowers from within the agencies concerned, the "sword of Damocles" of protected disclosures of abuses, are instrumental in assuring that legal limits placed on surveillance activities are in fact respected. It is striking that this point was made very forcefully during our first hearing in April 2014 by Mr Hansjörg Geiger, a former head of the German BND.

63. However, under current US legislation, Mr Snowden would face very serious espionage charges without being able to raise a public interest defence. At a time when the United States has been strengthening its whistle-blower protection laws for federal employees and industry (e.g. the finance sector), such that few if any private sector employees are excluded, the situation with respect the intelligence community has been schizophrenic. Between 2008 and 2012, intelligence community contractors connected to the Department of Defence (DEA and NSA, including those like Mr Snowden) would have had whistle-blower protection rights with jury trials as part of the National Defence Authorisation Act, but these were removed in 2013. Nonetheless, these protections related to retaliation or unfair treatment in employment and did not offer protection against criminal prosecution. In fact, the number of prosecutions of whistle-blowers has much increased under the Obama administration, which has charged a higher number of "leakers" – i.e. persons who revealed information to the American public, hardly the kind of "spies" targeted by the Espionage Act enacted in 1917, when the United States entered the First World War – than all the previous administrations combined.[39]

---

35. Doc. 13734, Recommendation 2067 (2015) and Resolution 2045 (2015).
36. *The Intercept*, 19 May 2014, "Data Pirates of the Caribbean: the NSA Is Recording Every Phone Call in the Bahamas".
37. *The Guardian*, 6 September 2013, "Revealed: how US and UK spy agencies defeat internet privacy and security".
38. *The Guardian*, 30 June, 2014, "New NSA leaks show how US is bugging its European allies".

64. The various whistle-blower protection provisions, which the Assembly referred to in Resolution 1729 (2010), seem of no avail to Mr Snowden. For instance, the US Whistleblower Protection Act of 1998 (WPA) explicitly excludes intelligence agents, while the separate Intelligence Community Whistleblower Protection Act (ICWPA) – enacted at the same time and covering employees and private contractors of the Central Intelligence Agency, the National Security Agency and other US intelligence services – neither includes any actual protections nor outlaws retaliation. Rather, it legalises disclosures and allows national security whistle-blowers to release classified information to a designated entity (the Office of the Inspector General, or the US Congress, via the Department of Justice), but not to the public, and covers only "urgent concerns".[40] Presidential Policy Directive 19 (PPD-19) of 10 October 2012 attempts to close the gap by providing protections to intelligence employees who report cases of "waste, fraud, abuse", but these were only extended to "employee[s] serving in an Intelligence Community Element". PPD-19 only applies to private contractors with respect to protecting them from security clearance retaliation and it does not appear to cover employees who report human rights violations. This directive carries the force of law, but it can be reversed at any time by the current President or one of his successors.

65. On 7 July 2014, President Obama signed the "Intelligence Authorization Act for Fiscal Year 2014", a statute that includes a section on the "Protection of Intelligence Community Whistleblowers". The provision specifies that intelligence agency employees who disclose information about possible misconduct within their agencies to designated entities (e.g. their superiors at the agency, one of the inspector generals or the House and Senate Intelligence committees) will be protected from retaliation. For the first time, intelligence agency employees can claim statutory protection as whistle-blowers if they suffer retaliation for co-operating with an investigation or testifying under oath.

66. While these protections are now codified into law by statute, they were not available at the time when Edward Snowden made his disclosures, and still do not apply to private contractors such as Mr Snowden's employer. Furthermore, some lawyers are concerned that, in practice, the law could fall short of its aims, because the internal reporting channels could instead be used to identify and punish potential whistle-blowers instead of actually addressing their concerns. *Deutsche Welle* pointed out that whistle-blowers can appeal to an administrative board under the new law if they believe they have been victim of retaliation for their disclosure, but there is no right to an independent due process hearing, and the board's members will all be selected by the Director of National Intelligence.[41] In addition, intelligence agency employees do not enjoy whistle-blower protections at all if they signed a non-disclosure agreement, and defendants cannot view the evidence against them if it is classified.

67. Yet, whistle-blowers remain indispensable as a last resort for the public to identify failures in accountability at the local, regional, national and even international level. The Snowden files have revealed the utter lack of transparency and democratic accountability in the stages of passing and implementing legislation (if any) that authorises State agencies to conduct mass surveillance. The United Nations High Commissioner for Human Rights, Ms Navi Pillay, credited Mr Snowden for starting a global debate on State surveillance powers, saying that "those who disclose human rights violations should be protected: we need them".[42] Ms Pillay stated that "we owe a great deal to him for revealing this information" that "go[es] to the core of what we are saying about the need for transparency, the need for consultation".

68. The June 2014 report of the Office of the United Nations High Commissioner for Human Rights, "The Right to Privacy in the Digital Age", took a position akin to the Council of Europe's on the need to encourage whistle-blowers to report human rights violations, corruption and fraud. It viewed the massive surveillance programmes that gathered information on emails, phone calls and Internet use by millions of ordinary people in many States as potential breaches of privacy. The report called for all branches of government, as well as completely independent civilian institutions, to be involved in the oversight of surveillance programmes to ensure that the same rights people have offline are also protected online. In a State where oversight

---

39. *The New York Times*, 23 September 2013, "Former F.B.I. Agent to Plead Guilty in Press Leak". Donald Sachtleben (FBI) was the eighth leak-related prosecution under the Obama administration, while only three such cases were prosecuted under all previous presidents; the latest case so far also concerns an official, Jeffrey A. Sterling (CIA), who was found guilty of espionage for having leaked information to the *New York Times* (see: "C.I.A. Officer Is Found Guilty in Leak Tied to Times Reporter", *The New York Times*, 26 January 2015 (www.nytimes.com/2015/01/27/us/politics/cia-officer-in-leak-case-jeffrey-sterling-is-convicted-of-espionage.html?_r=1).

40. For example "a serious or flagrant problem, abuse, violation of law or Executive order, or deficiency relating to the funding, administration, or operations of an intelligence activity involving classified information, but does not include differences of opinions concerning public policy matters", "Intelligence Community Whistleblower Protection Act," Section g.1.A.

41. *Deutsche Welle*, 10 July 2014, "Whistleblower law expands protection to US intelligence agents".

42. *The Guardian,* 16 July 2014, "Edward Snowden should not face trial, says UN human rights commission".

mechanisms over surveillance programmes are weak, inexistent or not sufficiently transparent, protected disclosures by whistle-blowers play an invaluable role in checking the security services' powers and ensure that serious human rights violations by State agents are not improperly shielded in the name of "State secret".

69. The case of John Kiriakou, who is so far the only CIA agent who spent time in prison because of the torture methods used in the "war on terror", which are described in detail in a recent report published by the US Senate,[43] is telling: Mr Kiriakou was imprisoned because he blew the whistle on "interrogation methods" such as waterboarding, which he could no longer tolerate. The message from prison that his lawyer, Ms Jesselyn Radack, herself a whistle-blower at the US Department of Justice, read out via live video link at the committee's meeting on 29 January 2015,[44] is deeply moving.

70. Following the disclosures by Edward Snowden and others, some States have ushered in legislative changes tending to discourage rather than encourage whistle-blowing. In Australia, for instance, new security laws adopted in September 2014[45] amount to an extreme crackdown on whistle-blowers and could affect journalists too. The legislation expands the powers of the Australian Security Intelligence Organisation (Asio) and includes the creation of a new offence punishable by five years in prison for "any person" who discloses information relating to "special intelligence operations". This person would face a 10-year sentence if the disclosure "endanger[s] the health or safety of any person or prejudice[s] the effective conduct of a special intelligence operation".

71. Such measures run counter to the Assembly's stance in favour of transparency, reconfirmed in Resolution 1954 (2013) on national security and access to information. In line with the Tshwane Principles endorsed by the Assembly in this resolution, I would encourage all States to consider putting into place a "public interest defence". According to Tshwane Principle 43, public personnel who are subject to criminal, civil or administrative proceedings because of disclosures that are not otherwise protected should still be able to raise a public interest defence under certain conditions. In order to verify the legitimacy of this defence, the prosecution and courts 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 had 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 governing the protection of whistle-blowers;

v. the existence of exigent circumstances justifying the disclosure.

72. I should like to stress that "public personnel" encompasses not only government agents, but also employees of private contractors or sub-contractors.[46]

4. The Council of Europe's own internal whistle-blowing channels – an example to follow?

73. In the wake of Assembly Recommendation 1916 (2010), the Secretary General of the Council of Europe promulgated Rule No. 1327 of 10 January 2011 on awareness and prevention of fraud and corruption. Rule No. 1327 makes it a duty for secretariat members "to report any reasonable suspicion of misconduct they deem to be fraud or corruption to the Director General of Administration or to the Director of Internal Oversight".[47] The creation of such an internal reporting channel is to be welcomed as a step towards enhancing transparency and governance in the Council of Europe itself.

---

43. See, for example, the ACLU's National Security Project's website: www.thetorturereport.org/.
44. "A law meant for spies is being used against whistle-blowers"; the ordeal of Mr Kiriakou, Ms Radack and Mr Drake (a former senior NSA official, see paragraph 86) is the subject of a TV documentary ("SILENCED – the war on whistle-blowers").
45. *The Guardian*, 26 September 2014, "Security laws pass Senate amid fears over 'draconian' limits to press freedom". "National security laws allow whistle-blowers to be jailed and give Asio sweeping powers to gather online data".
46. Or more precisely, any "persons employed by non-State bodies that are owned or controlled by the government or that serve as agents of the government; and employees of private or other entities that perform public functions or services or operate with substantial public funds or benefits, but only in regard to the performance of those functions, provision of services, or use of public funds or benefits" (Tshwane Principles, Definitions).
47. Rule No. 1327, Article 4.

74. Rule 1327 covers all members of the Council of Europe staff at any level, but also appointed officials and persons who participate in the Organisation's activities in different ways (including the judges of the European Court of Human Rights, the Commissioner for Human Rights, trainees, experts, consultants and employees of outside companies contracted by the Council of Europe).[48] A comparison with the European Commission's guidelines on whistle-blowing (SEC(2012)679), however, shows that there is some room for improvement in the Council of Europe's internal guidelines.

75. First, the Council of Europe's guidelines do not specify whether and under which conditions protection against retaliation also applies in cases where whistle-blowers resort to external channels to report reasonable suspicions of fraud or corruption. The European Commission's rules suggest that staff members first report serious irregularities to their immediate superior, director-general or head of service. As a second option, if the whistle-blower fears retaliation, the rules allow staff to report directly to the Secretary-General of the Commission or the European Anti-Fraud Office (OLAF). And thirdly, staff members can resort to external reporting as an option of last resort. Once OLAF or the Secretary-General receives the internal report, an indication must be given to the whistle-blower within 60 days as to the time required to take appropriate action. If no action is taken within that time or the whistle-blower can demonstrate that the time set is unreasonable in light of all the circumstances of the case, he or she is entitled to make use of the possibility of external whistle-blowing as provided for in the Commission's staff regulations. In addition, if "neither the Commission nor OLAF has taken appropriate action within a reasonable period, the staff member who reported the wrongdoing has the right to bring his or her concerns to the attention of the President of either the Council, the Parliament or the Court of Auditors, or to the Ombudsman", in which case whistle-blower protection continues to apply.

76. In my view, the Council of Europe should consider specifying the time frame in which a reply must be given to the whistle-blower and clarifying the conditions under which a whistle-blower can use external channels to report irregularities. The potential importance of external channels is highlighted by the fact that the Director General of Administration, as one of the addressees of the prescribed internal reporting mechanism, may well find himself or herself in a conflict-of-interest situation if the report concerns financial or other administrative abuses.

77. Also, Article 4.3 calls for reports of irregularities to be "where possible, substantiated by reliable information and documentation", which could place an unreasonable burden on the whistle-blower. The European Commission's position is more accommodating in that "staff members will not be expected to prove that the wrongdoing is occurring, nor will they lose protection simply because their honest concern turned out to be unfounded".[49] This position comes closer to the Tshwane Principles, which state in Principle 38 that "[a] person making a protected disclosure should not be required to produce supporting evidence or bear the burden of proof in relation to the disclosure".

78. Finally, the Council of Europe guidelines allow Secretariat members, when in doubt about whether an action constitutes fraud or corruption, to seek guidance and advice from the Director General of Administration or from the Director of Internal Oversight.[50] By contrast, the European Commission notes that experience suggests that early guidance and advice is best carried out by a point of contact not connected with the investigation function.[51] Because the directors take part in the investigative process later on, the Council of Europe should also consider attaching the guidance and support functions to another, independent body.

79. This said, the testimony before the Committee on Legal Affairs and Human Rights on 29 January 2015 of Maria Bamieh, former British prosecutor at EULEX in Kosovo,[52] shows that even the best guidelines do not prevent whistle-blowing from turning into a terrible ordeal for the person concerned, as long as the prevailing institutional culture does not truly value the contribution of whistle-blowers. As the investigation of Ms Bamieh's case, foreseen under the Commission guidelines, is still underway,[53] I prefer not to go into any more detail at this point.

---

48. Ibid., Article 2.
49. European Commission's SEC(2012)679, 6 December 2012 – Communication from Vice-President Šefčovič to the Commission on Guidelines on Whistleblowing, paragraph 3.
50. Rule No. 1327, Article 4.4.
51. European Commission's SEC(2012)679, op. cit., paragraph 5.
52. See press release of 30 January 2015, "A law meant for spies is being used against whistle-blowers".
53. In line with the Committee's decision on 29 January 2015, I asked the EU High Representative on External Relations, who oversees Eulex, for some explanations from the institutional point of view, but I have not yet received an answer.

5. Towards a convention to enhance whistle-blower protections across Europe and beyond

80. As indicated in the Assembly's earlier recommendation on whistle-blower protection, and in light of more recent developments, I should like to encourage States to engage in preparations for a binding legal instrument to further improve whistle-blower protection. Whilst the original title of the motion underlying this report favoured an additional protocol to the European Convention on Human Rights on the protection of whistle-blowers,[54] I would opt for a separate convention negotiated under the auspices of the Council of Europe, which would not require, as an additional protocol to the European Convention on Human Rights would, ratification by each and every State Party. Such a framework convention, to be completed and implemented by national legislation, could take into account the diversity of legal systems across the Council of Europe's member States. It should be designed to provide potential whistle-blowers with equivalent legal protection regardless of where they live or where they make a disclosure. The convention could build on the *acquis* reflected in the Committee of Ministers' recommendation. Its main benefit would be its legally binding character; such a convention could also be opened to interested non-European States and thereby contribute to promoting good governance and rebuilding public confidence on a global level.

81. In the drafting process, lessons could be drawn from recent developments, in particular concerning whistle-blowing in the field of national security. Moreover, States could consider granting asylum rights for whistle-blowers, especially when they leak sensitive information concerning one State, which also concerns other States, and possibly whilst residing in yet another State. Our expert, Ms Anna Myers, explained during the hearing before the committee in June 2014 the extent to which cross-border protection for whistle-blowers is needed in today's inter-connected world. A case in point is that of Mr Snowden, for whom it is particularly difficult to ensure that the concerns he raised, which are of interest to a number of countries, are properly investigated, especially if he were deported to the United States, where he would face serious criminal charges without being able to raise the public interest defence.

82. Independently of the unavoidably time-consuming negotiation process for a convention on the protection of whistle-blowers, I would urge States to grant asylum to any bona fide whistle-blower, who fulfils the criteria for whistle-blower protection applicable in the State considering asylum, and who is threatened with retaliation in his or her home country. The obvious question is whether Edward Snowden would qualify for whistle-blower protection under the standards advocated above.

6. A case in point: Edward Snowden

83. In the following, I should like to examine whether Edward Snowden's disclosures qualify for whistle-blower protection according to the principles developed above.

84. The first question is whether the information he disclosed was authentic and related to "wrongdoings". Governments have neither denied nor confirmed the existence of many of the surveillance techniques described in the files disclosed by Mr Snowden. But the information was never shown to be falsified or misleading in a way that would seriously put its authenticity and veracity into question. Also, the NSA's surveillance activities disclosed by Mr Snowden may well constitute human rights violations or abuses of public office.[55] In my report on "Mass surveillance", I have explained in some detail why these programmes violate, *inter alia*, the right to privacy.[56] Even if it turns out that the NSA had a legal basis for all its surveillance programmes, including those concerning US citizens who were not suspected of any wrongdoing, Mr Snowden had at least "reasonable grounds to believe that the information disclosed tends to show wrongdoing".[57] In believing that the NSA's mass surveillance programmes may violate the United States Constitution, Mr Snowden is in good company: at least one federal judge came to the same conclusion.[58] Most recently, in January 2015, the United Kingdom Investigative Powers Tribunal found in the case brought by Liberty and Privacy International that the secret intelligence sharing arrangements between the United Kingdom and the United States, known as Prism and Upstream (and disclosed with the help of Edward

54. See paragraph 3 above.
55. See Tshwane Principles (note 17), Principle 37.*b* and *g*.
56. Doc. 13734, paragraphs 79-94.
57. See Tshwane Principles (note 17), Principle 38.*a*.i.
58. Federal Judge Richard Leon in December 2013 characterised the NSA's metadata acquisition as an "almost-Orwellian technology" that likely represented a Fourth Amendment breach (see Volz, "The NSA's mass surveillance programme is about to go on trial", 4 November 2014, www.nationaljournal.com/tech/the-nsa-s-mass-surveillance-program-is-about-to-go-on-trial-20141103; and Doc. 13734, paragraph 70.

Snowden), did not comply with human rights laws (in particular Articles 8 and 10 of the European Convention on Human Rights) for seven years because the internal rules and safeguards supposed to guarantee citizens' privacy had themselves been kept secret.[59]

85. The second question is whether the disclosures qualify for protection despite the fact that Mr Snowden went public rather than limiting himself to internal channels. He shared confidential electronic files he had previously copied using his access as a contract worker for the NSA with a small number of journalists whom he had previously selected on the basis of their reputation as reliable and responsible individuals. According to the principles advocated by the Assembly,[60] public disclosures qualify for protection only as a last resort, after attempting to report concerns through internal channels.

86. During the hearing before the committee in June 2014, Mr Snowden explained that he reported his concerns about the NSA's mass surveillance programmes to colleagues and supervisors, both orally and by email. He said that colleagues to whom he explained certain new surveillance programmes were shocked, but did not do anything about it. The response he received was that the system is set up to bury problems, not to resolve them. In addition, Mr Snowden had observed closely that earlier NSA whistle-blowers, who had persisted in using internal reporting channels, did not benefit from any protection. Instead, they suffered from different forms of retaliation. Mr Thomas Drake, who had disclosed unclassified files to a newspaper after unsuccessfully reporting through internal channels on an inefficient programme wasting US$1.2 billion ended up being criminally prosecuted. Mr William Binney also tried to complain through official channels, only to have the Inspector General to whom he reported give his name to the Justice Department for criminal prosecution under the Espionage Act. These earlier NSA whistle-blowers did not succeed in triggering a wide public debate either. Because they had refrained from securing documentary evidence for their claims, they were treated as liars. These cases convinced Mr Snowden that he had no viable alternative reporting channel within the agency in order to have his grievances addressed.

87. The NSA has contested these assertions, claiming that Mr Snowden raised no such concerns vis-à-vis his superiors. Yet, the agency has refused to disclose communications Mr Snowden sent from his NSA account, except for a single email in which Mr Snowden sought a clarification on laws governing the NSA's activities but did not make reference to bulk data collection or concerns about violations of privacy. A journalist submitted a Freedom of Information Act (FOIA) request to seek the disclosure of emails sent from Mr Snowden's NSA account in the first five months of 2013. But the NSA responded that it could not release emails sent by Mr Snowden because doing so would invade his "personal privacy", which is covered by the sixth exemption under the FOIA that allows refusing the disclosure of information that would constitute a "clearly unwarranted invasion of personal privacy.[61] Other reasons given for refusing to release these messages were that they are being compiled for law-enforcement purposes and that their publication would interfere with the proceedings; that they could reveal the identities of confidential sources; and that they would reveal law-enforcement techniques and procedures. Mr Snowden has since argued that the NSA's publication of a single email was a "clearly tailored and incomplete leak" that did not reveal the multiple written and verbal concerns he had repeatedly raised before the NSA.

88. The NSA has taken an equally nebulous approach to the exponential increase of FOIA requests it has received following the Snowden disclosures. Since 6 June 2013, the office has received over 5 200 requests for the publication of classified information; for the same period in the previous year, the NSA had received just over 800 such requests. According to *The Guardian*,[62] the NSA has refused to entertain demands from private citizens about whether the agency stored their metadata, giving a "Glomar response" (neither confirm nor deny), while stressing the legality of the surveillance programmes. This persisting lack of transparency surrounding surveillance programmes makes whistle-blowers crucial as the only sources of information to verify that the agencies are working within legal bounds. To sum up, it would appear that Mr Snowden had no viable internal reporting channel at his disposal other than the attempts he had made of raising his concerns with immediate colleagues and superiors.

89. In addition, the claim to protection of Mr Snowden's public disclosures depends on whether he only disclosed the amount of information that was reasonably necessary to bring to light the wrongdoing, and that he reasonably believed that the public interest in the information revealed outweighed any harm to the public interest that would result from the disclosure.[63]

---

59. Ruling available on the IPT website; see *The Guardian*, 6 February 2015, "'Trust us' mantra undermined by GCHQ tribunal judgment. The judgment rules that secret intelligence sharing arrangements between Britain and the United States did not comply with human rights laws".
60. See, for example, Tshwane Principles (note 17), Principles 38-40.
61. *US News*, 14 July, 2014, "NSA: Releasing Snowden Emails Would Violate His Privacy".
62. Jason Leopold, Top NSA officials struggled over surge in FOIA requests, emails reveal, *The Guardian*, 29 May 2014.

90. Regarding the first point, matters are complicated by the fact that Mr Snowden acted under extreme time pressure. Once he accessed the sensitive data in question, he was in danger of being caught out by the NSA, and consequently being no longer able to prove his allegations. He was obliged to flee from the United States. When he left, he did not yet know where he would end up finding protection. But he was aware of the fact that the data he had copied in bulk could not all be made public, let alone fall into the hands of the services of a foreign power, without causing damage to national security. Edward Snowden, in both hearings before the committee in April and June 2014, described himself as an American patriot who wanted to defend the United States Constitution as well as the privacy of people even outside the United States. He did not in any way intend to endanger legitimate national security interests or assist the enemies of freedom. In order to minimise such risks, he had made arrangements with trusted, responsible journalists working for what he called "respected journalistic institutions" such as *The Guardian* and *The New York Times* to take custody of the data he had copied in bulk, on condition that these journalists would independently assess, if need be in consultation with the authorities, which of these data could be published without endangering legitimate national security interests, and which ones could not.[64] It would appear that the selection made by the journalists to whom Mr Snowden had entrusted the data is fairly responsible – so far, the NSA has not been able to pinpoint any actual damage to national security interests caused by the publication of data leaked by Mr Snowden through the journalists to whom Mr Snowden had, out of necessity, delegated the selection of the materials that should be published in the public interest.

91. The second condition, namely that Mr Snowden reasonably believed that the public interest in the disclosure of the information outweighed any harm resulting from disclosure would appear to be fulfilled, too. The programmes and techniques that allow the NSA and other intelligence agencies to engage in bulk collection and analysis of personal data around the world would not have come into the public domain without the publication of the files with the help of Mr Snowden. This was clearly of interest to the American public as well as the people of numerous other countries targeted by the mass surveillance and intrusion programmes exposed. The strong media interest in the disclosures, as well as the numerous parliamentary and other public inquiries at the national level,[65] in the framework of the United Nations,[66] the European Parliament[67] and last but not least by our own Assembly show the extent of public interest in the concerns raised by Mr Snowden. The ensuing debate has already triggered some legislative changes, and I can only hope that the Assembly's recommendations on the basis of the parallel report on "Mass surveillance" will lead to further national and international action aimed at setting up and enforcing an appropriate legal framework and technical protection measures to reconcile legitimate national security concerns with the fundamental human right to privacy.

92. Finally, the harm caused to the public interest in protecting the legitimate activities of the intelligence and security services as a result of Mr Snowden's disclosures does not appear to outweigh the tremendous contribution the disclosures have made to the debate on the need to protect privacy and hold intelligence services to account. The US authorities initially claimed that Mr Snowden's leaks had endangered the lives of secret agents, though they never provided any specific information allowing this claim to be verified. In any event, the government itself has routinely leaked information on secret agents for political advantage.[68] During the hearing before the committee in June 2014, Mr Snowden responded to allegations that his disclosures diminished the ability of intelligence agencies to effectively combat terrorism and organised crime as follows:

93. First, the mass surveillance programmes discussed today were never shown to be effective to begin with. This was the conclusion, for example, of the Privacy and Civil Liberties Oversight Board (PCLOB).[69] The PCLOB criticised the NSA's telephone records programmes as having provided "minimal" benefits in stopping terrorism and having led to "no instance in which the programme directly contributed to the discovery of a previously unknown terrorist plot or the disruption of a terrorist attack".[70] Although the PCLOB, in its report to

---

63. See Tshwane Principles (note 17), Principle 40.*b* and *c*.
64. Luke Harding, The Snowden Files, *The Guardian publications*, 2014, passim.
65. Doc. 13734, paragraphs 70-77.
66. "The right to privacy in the digital age", Report of the Office of the United Nations High Commissioner for Human Rights, document A/HRC/27/37: www.ohchr.org/Documents/Issues/DigitalAge/A-HRC-27-37_en.doc; UN General Assembly Resolution 68/167 of 18 December 2013 on "The right to privacy in the digital age": www.un.org/ga/search/view_doc.asp?symbol=A/RES/68/167.
67. See Doc. 13734, paragraphs 108-109. A follow-up report is currently under preparation in the European Parliament.
68. Committee on Legal Affairs and Human Rights, Hearing on "Improving whistle-blower protection" , 24 June 2014.
69. The Board is an independent, bipartisan agency within the executive branch, established by the Implementing Recommendations of the 9/11 Commission Act, Pub. L. 110-53, signed into law in August 2007, see its website at: www.pclob.gov/.
70. The *New York Times*, 23 January 2014, "Watchdog report says N.S.A. Program is Illegal and Should End".

President Obama in January 2014, ended up finding most of the surveillance programmes legal, it has expressed doubts as to the proportionality of the surveillance in relation to its meagre results. These doubts have grown following the publication, in June 2014, of information following which nine out of the ten communications intercepted under these programmes were not those of legitimate surveillance targets but those of ordinary American and foreign Internet users not suspected of any wrongdoing.[71]

94. Second, Mr Snowden pointed out that the public, and in particular criminals, have always known about telephone wiretaps, but criminals all over the world still use telephones. Similarly, we now know of Internet surveillance, yet continue to use the Internet and send emails on a daily basis. It is also untrue that the disclosures have disrupted the NSA's operations. Even after the disclosures by Mr Snowden, reports of continuing surveillance programmes have emerged – at least some of them still seem to be operating. Revealing that the NSA engages in online surveillance is not likely to push terrorists and criminals to completely forego online communications and even so, the NSA still has the possibility of using traditional means of tracking and analysing such targets' activities.

95. Finally, as Mr Snowden explained drawing also on his experience as a former CIA agent, the kind of disruption that the revelations may have introduced into terrorist communications networks is not damaging the fight against terrorism; disrupting criminals' usual modes of communications causes them to make more mistakes, which can be used to analyse and understand their new patterns of communication.

96. It is true that the Snowden revelations have caused huge embarrassment and political and diplomatic complications for the United States and some other countries. But in my view, these cannot be held against Mr Snowden: they are the consequences of the actions taken by the NSA and its allies. It is the act of spying on friends and allies that has given rise to their adverse reactions,[72] not the revelation of this information. Watergate was a disaster for the Nixon presidency – because he had authorised the burglary, not because it became publicly known. Edward Lucas, a strong critic of Mr Snowden (and, in my view, a particularly credible journalist), is wrong when he blames the messenger for the damage done to transatlantic relations.[73] Much of the public relations damage caused by the Snowden affair (and the corresponding propaganda gains for Mr Putin's Russia) is self-inflicted: by persecuting Mr Snowden in such a ruthless way, including death threats by senior officials,[74] the US Government chose to play the role of the international villain, and by failing to engage in a meaningful dialogue with its allies on ways and means to restore trust, it further increased the diplomatic fallout from the disclosures. I much regret the public relations present that this affair provided for Mr Putin, but this can hardly be blamed on Mr Snowden.

97. I also agree with Mr Snowden in that it does not really help terrorists and organised criminals to know for sure that their communications may be monitored: the most dangerous criminals were always aware of the risk of surveillance and tried to shield themselves – more or less successfully in the face of constantly evolving surveillance methods. And, as Mr Snowden said in light of his own professional experience, the vast majority of terrorists and other criminals are rather unsophisticated, if not primitive individuals. They will keep making mistakes enabling the authorities to catch up with them. The need for communication does not go away, and if criminals communicate less for fear of being monitored, they will be less effective criminals. Personally, I find these arguments quite convincing, and I do believe that Mr Snowden, too, could "reasonably believe" that the public interest in having the information revealed outweighed any harm resulting from disclosure.

98. In sum, Mr Snowden's public disclosures should be considered as protected and Mr Snowden should enjoy protection against any retaliation. In particular, he should not be subject to criminal proceedings for the disclosure of classified or otherwise confidential information.[75] According to the rules on whistle-blower protection put forward in this report, Mr Snowden would not even need to raise the "public interest defence".[76] As explained above,[77] this defence is a safeguard that should be at the disposal of a public servant who is subject to criminal proceedings or other sanctions for having made a disclosure that is *not* otherwise protected – he or she can invoke the defence if the public interest in disclosure of the information in question outweighs the public interest in non-disclosure. If Mr Snowden could not, for example, show that he first attempted to use

---

71. *The Washington Post*, 5 July 2014, "In NSA-intercepted data, those not targeted far outnumber the foreigners who are".
72. Doc. 13734, paragraphs 104-106.
73. Edward Lucas, The Snowden Operation, Inside the West's Greatest Intelligence Disaster, 2014.
74. *Huffington Post*, 26 January 2014, "Edward Snowden: There are 'significant threats' to my life"; tech dirt of 3 October 2013; "Former NSA Director jokes about putting Snowden on a 'kill list', says he 'hopes' that NSA is involved in targeted killings".
75. Tshwane Principles (note 17), Principle 41.A.1.
76. Tshwane Principles (note 17), Principle 43.
77. At paragraph 71.

available (and viable) internal reporting channels, he could still avail himself of the public interest defence although it would then be up to the prosecutorial and judicial authorities to determine whether the public interest in disclosure actually outweighs the public interest in non-disclosure, taking into account all relevant circumstances,[78] including whether the extent of the disclosure was reasonably necessary. In my view, it was.

99. In the United States, Mr Snowden is still threatened with heavy-handed criminal prosecution under provisions of the Espionage Act with the possibility of life in prison with no perspective of early release. The Espionage Act enacted in 1917 was applied very sparingly, and only three times for the prosecution of officials who leaked confidential information until the beginning of the Obama administration (against Daniel Ellsberg and Anthony Russo in 1973 for publishing the "Pentagon Papers" – the latter prosecution ended in a mistrial; against Samuel Morison in 1985 for publishing information on a Soviet naval build-up as a "wake-up call" for the American public, and in 2005 against Lawrence Franklin, for passing information on the Iranian nuclear programme to congressional lobbyists).[79] But the 1917 Espionage Act has recently been used far more frequently, and in relation not to traditional espionage as in most previous cases, but to punish leaks to mainstream media. Out of a total of 12 prosecutions against officials accused of providing secret information to the media, nine have occurred since President Obama took office.[80] These include the above-mentioned NSA whistle-blowers Thomas Drake and Chelsea (formerly Bradley) Manning, who leaked numerous documents through Wikileaks, and most recently the cases of Edward Snowden, Donald Sachtleben and Jeffrey A. Sterling. The 1917 Espionage Act does not allow for any form of public interest defence. This means that Mr Snowden, if he were to return to the United States, would face very serious punishment. In line with the recommendation made above, I would therefore strongly plead for granting Mr Snowden asylum in any of the European States which have benefited from the disclosure of NSA surveillance targeting their citizens, their businesses and even their elected political leaders.

100. In a post-script to this case study, I should like to address allegations that Mr Snowden is wittingly or unwittingly "in league" with the Russian FSB. The strongest and most credible case is made by Edward Lucas, who argues that Mr Snowden was recruited by Russian intelligence under a "false flag", i.e. that he was manipulated by agents posing as Internet privacy activists and nudged into his actions by making use of the somewhat "muddled" views he had uttered on the Internet when he was working for the CIA. Drawing a parallel with Western peace protesters during the Cold War, Mr Lucas argues that Mr Snowden acted as a "useful idiot" by effectively sabotaging Western intelligence efforts whilst believing that he was helping the cause of privacy. In a similar vein, ex-KGB Major Boris Karpichkov said spies from Russia's SVR (foreign intelligence service) posing as diplomats tricked Snowden, whom the SVR had considered as a potential defector since his CIA posting in Geneva, into seeking asylum in Russia. Mr Karpichkov believes that the Kremlin will keep Mr Snowden for another three years, until he has no more information to give, because it wants to know exactly how America and Britain encrypt and decrypt secret information.[81] Ex-KGB General Oleg Kalugin, who purportedly still has contacts with the FSB, claimed that the Russians were "very pleased with the gifts Edward Snowden has given them" in exchange for staying in Russia. He went as far as saying that Mr Putin got everything Mr Snowden accessed, including military documents, despite Mr Snowden's claims that he handed all files to journalists prior to leaving Hong Kong and had not kept any of the confidential information when he entered Russia. Finally, former director of CIA operations Jack Devine was of the opinion that it would be "most unusual if he [Snowden] were allowed to remain there [in Russia] as a guest for free".[82]

101. But it should be noted that the two former KGB agents are defectors now living in the United Kingdom and the United States respectively, and may well be motivated by wishing to please their Western handlers. Mr Devine's opinion is purely speculative. Also, Mr Snowden's presence in Moscow has public relations benefits for the Kremlin whether or not he discloses any secrets to the SVR. I should also like to recall that Mr Snowden pointed out during the hearing before our committee in June 2014 that he had initially travelled to Moscow for purposes of transiting to Latin America. He ended up stuck in Moscow because the United States had revoked his passport and none of his more than 20 asylum applications for countries other than Russia was accepted.[83] For argument's sake, even if Mr Snowden was tricked by Russian intelligence into making

78. Tswhane Principles (note 17), Principle 43.*b*.i to v.
79. Jim Snyder, The Espionage Act, A spy-fighting tool is now aimed at U.S. leakers, Bloomberg Quick Take, 3 October 2014: www.bloombergview.com/quicktake/the-espionage-act.
80. Ibid. and the *Tampa Bay Times*, The Pundit Fact, "CNN's Tapper: Obama has used Espionage Act more than all previous administrations".
81. *The Mirror*; 7 July 2014, "Edward Snowden was targeted by Russian spies 6 years before he exposed US secrets".
82. Ibid.
83. *Business Insider*, 27 May 2014, "Two Top Cold War Spies Made The Same Troubling Prediction About Edward Snowden".

the disclosures in question: his actions were still motivated by the idealistic goal of protecting the right to privacy by exposing the NSA's mass surveillance and intrusion programmes. I should also like to recall that under Tshwane Principle 38.*b*, the motivation for a protected disclosure is irrelevant except where it is shown that the person making the disclosure knew that the information disclosed was untrue.

102. Ultimately, the focus of the discussion should not be placed on whether Mr Snowden is a hero or a traitor, but on whether the concerns he raised through his disclosures are well founded and what measures should be taken to address the problems raised through the NSA files and rebuild trust among allies and more generally in the safety of legitimate communications.

7. Conclusion

103. We have seen that some progress has been made since the Assembly's first report on whistle-blower protection, in particular in raising the general awareness of the important contribution whistle-blowing makes to transparency and accountability, in both the public and private sectors. Intergovernmental bodies such as the G20 and the OECD and also the Council of Europe's own Committee of Ministers have joined NGOs such as Transparency International, Public Concern at Work or the Whistleblower International Network, who had been campaigning for better whistle-blower protection for a long time. The case law of the European Court of Human Rights also deserves special attention: States should heed the principles established by the Court in cases concerning different countries and not wait until they are themselves found to be in violation of the Convention.

104. We have also seen that the existing legislation and international instruments are not yet sufficient to provide the effective protection whistle-blowers deserve. This is especially true for whistle-blowers working in national security-related fields, who are at present mostly excluded from the general whistle-blower protection rules. As the revelations enabled by Edward Snowden and a number of other, less prominent whistle-blowers have shown, there is no reason to believe that the security sector has less need for whistle-blowing for upholding good governance and accountability than any other parts of the public sector. As explained in the report on mass surveillance, the "Sword of Damocles" of an insider blowing the whistle on abuses could well be the most effective way to deter and sanction violations, given the notoriously weak parliamentary and judicial supervision mechanisms in most countries. The short "case study" on Edward Snowden provides an additional illustration of the issues in play. The resulting conclusions and recommendations for improvements – in particular the call for the negotiation of a Council of Europe convention on the protection of whistle-blowers – are reflected in the draft resolution and recommendation preceding this report.