Submission of Dr. Ashley Savage to the Intelligence and Security Committee of Parliament: Privacy and Security Inquiry

---

Executive Summary

This response seeks to outline concerns relating to the provision of whistleblowing mechanisms for employees in the UK security and intelligence community. In doing so it suggests that the effective provision of such mechanisms is a safer alternative to unauthorised leaking for the employee, the organisation, and national security as a whole. The response recognises that circumstances may arise where public disclosure may be the only viable option and recommends consideration of a new codified necessity defence to the Official Secrets Act 1989. The response outlines what would be required to include intelligence employees in the Public Interest Disclosure Act 1998. Ultimately, the response suggests that the Committee could do more to consider the position of whistleblowers in the security and intelligence services. Whether it be at a minimum: by regularly taking evidence on current arrangements and engaging in an audit of those arrangements, or at a maximum, by providing clearly defined direct access for employees to raise concerns with the committee as a top tier whistleblowing mechanism.

Biography

1. I am currently Senior Lecturer in Law and Programme Leader for the Information Rights LLM, at Northumbria University, Newcastle-Upon-Tyne. In 2012, I successfully completed a doctoral thesis at the University of Durham entitled: "Crown Servants and Unauthorised Disclosures: Whistleblowing, Executive Accountability and the Public Interest." The thesis considers the position of employees in the Civil Service, the Security and Intelligence Services and Armed Forces who raise concerns about wrongdoing or malpractice in the workplace. The research was conducted using publically accessible information. I am currently in the process of writing a monograph entitled 'Leaks, Whistleblowing and the Public Interest: The law on unauthorised disclosures' (for Edward Elgar publishing) which seeks to provide a comprehensive treatment of the law in the United Kingdom with reference to various accountability mechanisms and comparative material. I was previously employed as a helpline adviser for the charity, Public Concern at Work which provides a free advice line for whistleblowers. I was called to the bar by the Honourable Society of Grays Inn in 2010.

Introduction

2. It can be observed that intrusive electronic surveillance and data collection can, and will, most likely interfere with an individual's right to respect for private and family life, enshrined in article 8 ECHR.[1] The interference may be justified in the interests of national security, or the prevention or disorder or crime (or under any of the exceptions contained in art.8 (2) ECHR). Public authorities have obligations from the time the data is obtained to the way in which it is used and stored. Such interference may be regarded as disproportionate where data is collected on mass. The motivation for these activities requires consideration of the national security risks and whether these risks outweigh the potential harm caused by

[1] A matter discussed further in my response to the Joint Select Committee on the Draft Communications Data Bill, written evidence published 11th September 2012.

privacy intrusion. In determining whether this balance is being struck correctly, it is vital that those tasked with accountability, namely the Intelligence Services Commissioner, the Interception of Communications Commissioner and ultimately the Intelligence and Security Committee monitor these activities whilst allowing the intelligence services to operate effectively. Whilst it is acknowledged that the focus of the Committee's call for papers is on the balance between privacy and security, it is suggested that recent unauthorised disclosures by Edward Snowden also need consideration. The leaks identify the extent to which electronic communications are being monitored and the potential risks posed by unauthorised disclosures. It is noted that legal proceedings are ongoing and that there could be further revelations. Instead of providing specific comment on the legality of the Snowden leaks, I shall provide my views pertaining to both the law relating to unauthorised disclosures in the United Kingdom and the current mechanisms and legal protections afforded to whistleblowers in the security and intelligence services.

3. Whistleblowers can identify breaches of law or policy which may be difficult for accountability and oversight mechanisms to otherwise detect. Whilst it is not suggested that employees of the security and intelligence services, or employees in any work setting should be actively engaged in raising concerns outside of their organisation without actively attempting to rectify matters internally, circumstances may arise where the employee needs to go outside of the organisation. Providing visible and viable access to official mechanisms must be seen as preferable to unauthorised leaking, even when the subject of the leaks has later proved beneficial to oversight bodies. The United Kingdom has experienced a number of unauthorised disclosures resulting in criminal action over the past few years, but is yet to experience a leak on the scale of either the Bradley Manning or Edward Snowden revelations. Acts of leaking can never be completely prevented, however, reliance upon the Official Secrets Act 1989 is not sufficient to deter such acts from taking place. The United Kingdom needs to provide clear and effective alternatives.

The risks versus the rewards of unauthorised leaking

4. It is recognised that the Snowden leaks have fuelled international debate as to the way in which intelligence agencies monitor activities on the internet. It is clear that had the disclosures not been made, such public debate would not have taken place. It is acknowledged that a number of world leaders, Parliamentary bodies as well as campaign groups have expressed their concerns as to the nature of the activities undertaken. To the observer, it would appear that the activities are disproportionate to the purported aim.

5. The associated difficulty is that security and intelligence organisations are best placed to make a determination of what constitutes information harmful to national security and what does not. This places news organisations in a position where they are required to make a judgement as to whether it is safe to publish the material. Whilst they have access to the DA Notice Committee, this should be viewed in the context of a changing world whereby advancements in technology have replaced a few hastily photocopied documents with the potential to leak thousands of documents using portable storage devices or a CD rom. Moreover, advancements in technology have resulted in advancements in citizen journalism. Traditional media outlets can be bypassed altogether.

6. Unauthorised disclosures of official information pose a definite risk to the employee, who will likely face either most severe outcome resulting in prosecution, to the least severe, resulting in dismissal and loss of security clearance. The risk posed to the organisation will always be more difficult to quantify. What is apparent is that when unauthorised disclosures

reach the public domain they become accessible to all – friend and foe alike. Seemingly innocuous information which may not be considered harmful, either by the original leaker, an editor making a decision to publish, or the majority of the general public, may be extremely useful to the minority with harmful intent. Whilst it is recognised that circumstances may arise where an employee has no option but to go public, the safest way for both the employee faced with an issue of conscience and the organisation is for the employee to raise concerns using official whistleblowing mechanisms.

Whistleblowing arrangements for intelligence and security employees.

7. In 2010 the UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism made the following recommendations of best practice in relation to employees of the security and intelligence services. The report provides guidance which may be of use to the committee. Of particular relevance is Practice 18:

> "There are internal procedures in place for members of intelligence services to report wrongdoing. These are complemented by an independent body that has a mandate and access to the necessary information to fully investigate and take action to address wrongdoing when internal procedures have proved inadequate. Members of intelligence services who, acting in good faith, report wrongdoing are legally protected from any form of reprisal. These protections extend to disclosures made to the media or the public at large if they are made as a last resort and pertain to matters of significant public concern."[2]

In the following paragraphs I will seek to identify several concerns relating to the situation in the United Kingdom and potential avenues for further review.

Concern reporting procedures

8. There is very little publically available information as to the current concern reporting arrangements available to employees of the security and intelligence services in the United Kingdom**.** From Hansard and media reporting of the time we know that an independent staff counsellor was established in 1987**.** Since the Intelligence and Security Committee was established there has been no mention of the role of concern reporting mechanisms (at least in the publically available versions) until the 2007-2008 Annual Report. The Committee identified that The Security Service had established an 'Ethical Counsellor.' In this report the Committee welcomed the establishment of the post and also stated that in the absence of an equivalent post within SIS or GCHQ staff could approach the Staff Counsellor available to employees of all three services. Unfortunately, in subsequent reports there has been no further mention as to the activities and work of the Counsellors. It is acknowledged that these mechanisms may be working well. However, is recommended, that if the ISC are not doing so already, they should take evidence on what the current procedures are and how

[2] Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin, Compilation of good practices on legal and institutional frameworks and measures that ensure respect for human rights by intelligence agencies while countering terrorism, including on their oversight (2010), Practice 18. http://daccess-dds-ny.un.org/doc/UNDOC/GEN/G10/134/10/PDF/G1013410.pdf?OpenElement

they are working in practice and report on this. In contrast to allied jurisdictions such as the United States, very little information is provided on the United Kingdom's arrangements. The National Audit Office has recently conducted an exercise looking at the whistleblowing arrangements in central government departments, the report of which may be of use to the Committee.[3]

9. In *R v Shayler* Lord Bingham indicated that *Shayler,* amongst other options available, could have approached the secretariat to the ISC. Whilst it is acknowledged that the ISC has a secretariat, whether this provides an appropriate avenue for employees to raise concerns is less clear. In order to make an 'authorised disclosure' for the purposes of s.7 Official Secrets Act 1989, a Crown servant must make a disclosure "in accordance with his official duty." A defence is provided where the Crown Servant "believed that he had lawful authority to make the disclosure in question and had no reasonable cause to believe otherwise." There is no publically available information as to whether internal documentation or policy in the security and intelligence services authorises such disclosures to the Secretariat. If there is not a formal system in place already, the ISC may wish to consider whether it would be appropriate to have a system in place for receiving whistleblowing disclosures. This could be included, for example, in a staff whistleblowing policy. The ISC may also wish to consider whether s.7 should be amended to include a specific provision authorising disclosures to them. Whilst it would be generally most appropriate to keep whistleblowing disclosures within the organisation or outside the line management chain to the staff counsellor or equivalent, it would provide a controlled 'avenue of last resort' to account for situations whereby the employee felt unable to raise the concern internally or to the counsellor because of the nature of the issue concerned. It would also account for circumstances where the employee had raised the concern already and had felt that the matter had not been taken seriously. A disclosure of information to the ISC would be ultimately less harmful than an uncontrolled disclosure to the public domain.

Legal Protection for Raising Concerns

10. Currently, employees of the security and intelligence services are not protected by the whistleblowing legislation generally available to workers in all sectors of the United Kingdom. The United Kingdom is not compliant with the best practice suggested by the UN Special Rapporteur. Furthermore, it is lagging behind allied jurisdictions such as the United States which does provide protection against reprisals. Whilst it is acknowledged that whistleblowing protection laws in the United States have been ineffective, there have been reforms in this area. One must question whether it is acceptable for allied nations to provide whistleblowing protection laws where our own nation does not. This should be considered in the light of the nature of the information shared by the agencies and the collaborative nature of some activities. The Public Interest Disclosure Act 1998 and protection for whistleblowers in general has been recently the subject of review by the newly established Whistleblowing Commission and by the Department for Business Innovation and Skills. It is therefore an appropriate time to consider whether the legal provisions afforded by PIDA could be extended to the security and intelligence services.

11. In principle, Public Interest Disclosure Act is sufficiently flexible to allow for disclosures by intelligence employees. In order to be a legitimate instance of whistleblowing under PIDA,

[3] National Audit Office webpages, see also, the assessment criteria:
http://www.nao.org.uk/report/government-whistleblowing-policies/

the person must make a 'qualifying disclosure' which is in the public interest. The categories of information protected extend to information regarding: (i) a criminal offence, (ii) a failure to comply with any legal obligation, (iii) a miscarriage of justice, (iv) danger to the health and safety of any individual, (v) damage to the environment, (vi) or the deliberate concealment of information tending to show any of the matters listed above.[4]

12. As I recently identified in a co-authored response to a consultation by the Whistleblowing Commission, intelligence employees do have the right to take Employment Tribunal claims.[5] There are also procedures which provide for closed hearings so that national security information may be considered.[6] Despite this, there are three potential barriers to providing intelligence employees access to the Public Interest Disclosure Act. Firstly, the stepped disclosure regime offers protection to those who make 'wider disclosures' to the public domain. Any public disclosures made by intelligence officials are likely to be in breach of the Official Secrets Act 1989. A public interest defence could be added to the existing provisions contained in the Official Secrets Act 1989.

13. It is not suggested that a defence be added to open the floodgates for national security information to be leaked to the public domain, instead the defence could be limited to circumstances where serious matters have already been raised and the persons in receipt of the disclosures have failed to act, or in circumstances where there is an immediate risk to life. The Canadian Security of Information Act 2001 provides a good example of how such a provision could work. Section 15 of the Act requires a court weigh up the public interest of the disclosure against the public interest in non-disclosure. The provision ordinarily requires for prior disclosure to the Attorney General, the Security Intelligence Review Committee or the Communications Security Establishment Commissioner. Public disclosures can be made where the worker has not received a response in a reasonable time or in exigent circumstances, effectively providing a necessity defence. In *R v Shayler*, it was acknowledged that a necessity/duress of circumstances defence could be applied to the Official Secrets Act 1989, this has yet to be tested in court.

14. The second barrier relates to disclosures which may be made to prescribed persons under the Act. Prescribed persons, most often regulators or organisations performing a regulatory function are added to the list by way of a statutory order. Procedures may need to be implemented to ensure that disclosures which pertain to national security matters can be handled appropriately. Furthermore, it is suggested that it would be appropriate to add the Intelligence Services Commissioner and the Interception of Communications Commissioner to the list. It is noted from their annual reports that both Commissioners already engage in dialogue with staff from the security and intelligence services. It would therefore seem to make sense to provide whistleblowing protection to those whom raise concerns with the Commissioners. Furthermore, circumstances may result where, in the course of an inspection visit, an employee needs to raise a concern with the respective Commissioner. They should be protected from reprisal for doing so.

[4] Section 43B PIDA.

[5] As per s.191 and 193 Employment Rights Act 1996. R.Hyde and A.Savage, *Response to the Whistleblowing Commission*, 2013.

[6] Rule 54, Schedule 2 Employment Tribunals (Constitution and Rules of Procedure) Regulations 2004.

15. The third barrier relates to a remedy contained in the Public Interest Disclosure Act which provides the scope for an order of reinstatement to be made. The reinstatement of an employee who has made an unauthorised disclosure to the public domain may be an unrealistic proposition. The relationship of trust between the organisation, the employee and their co-employees is likely to be irreparably damaged. It may be sensible to limit the availability of remedy to financial compensation, however this should be the subject of consultation prior to recommendation.

16. If the above barriers could not be removed (for example, if it was considered unsuitable for a public interest defence to be inserted into the Official Secrets Act 1989) it is suggested that either a sector specific provision could be added to the existing Public Interest Disclosure Act, limiting the avenues of disclosure to officially authorised channels, or a new law could be introduced specifically for intelligence employees. If there is insufficient buy-in for the provision of an employment law, procedures could be implemented to protect employees from reprisal. This could include the prevention of disciplinary action against employees for raising concerns through prescribed channels and disciplinary action for those who react by responding with detrimental treatment.

17. A minimum reform, if this has not been done already, would be to develop memoranda of understanding with the security and intelligence agencies for the provision of an internal whistleblowing policy providing agreed procedures for access to the Intelligence Services Commissioner, the Interception of Communication Commissioner and the Intelligence and Security Committee. It is most apparent from the Committee's latest annual report that there is a desire to engage more closely with the services. It should be identified that even if reporting mechanisms are robust emphasis must also be placed on the culture of the organisation. The Committee's increased powers introduced by the Justice and Security Act 2013 pave the way for the Committee to become an official whistleblowing mechanism, the last resort before uncontrolled public disclosure. If the provision of whistleblowing mechanisms and protections such as the ones outlined in this response are considered to be unworkable or part of a longer term aspiration, in the immediate future the Committee should still take evidence on existing procedures and the culture of the organisations concerned.

18. I would be delighted to assist the committee further on any of the matters raised in this response.