courage.contact@couragefound.org
www.couragefound.org

03/05/2017

courage.contact@couragefound.org

Protection of Official Data

Consultation response from the Courage Foundation

The Courage Foundation provides support to individuals who have made important contributions to the historical record and find themselves in legal jeopardy for doing so. In particular we run the official public defence fund for NSA whistleblower Edward Snowden. Courage welcomes the opportunity to contribute to the current consultation on the Protection of Official Information.

In our opinion, the Law Commission's report represents a missed opportunity to bring the legislation concerning disclosure of official information into the digital age. Over the past decade, there have been a series of unauthorised disclosures of significant public importance, which have greatly informed public debate internationally – not least in the fields of diplomacy, intelligence and international taxation.

The prominence of these disclosures has been matched by concern at the treatment experienced by whistleblowers, including draconian criminal sanctions and long prison sentences.[1] We note that the European Commission is currently running its own consultation on the feasibility of instituting Union-wide whistleblower protection standards.[2]

The last time a full-scale inquiry into the law in this area was carried out, the Franks Committee received evidence from 114 witnesses including many from civil society and the news media.[3] We note

1 The most prominent case might be that of Chelsesa Manning, who was sentenced to 35 years' imprisonment under the Espionage Act in the United States and had her "clearly disproportionate" sentence commuted by President Obama in one of his last acts in office.

2 Public Consultation on Whistleblower Protection: http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=54254

3 Departmental Committee on Section 2 of the Official Secrets Act 1911 (September 1972). Cmnd. 5014 (hereafter Franks) ¶ 15

that concerns have been expressed about the extent and breadth of the pre-consultation carried out by the Law Commission in preparation of its own report.[4] We share these concerns and think it is important that there is further consultation before draft legislation is laid before Parliament.

Our recommendations are as follows:

i. It is important that the full range of voices are heard in this consultation. We suggest that an interim report and further consultations with civil society, media groups and other interested parties be undertaken before draft legislation is produced.

Espionage Clauses

ii. Although the legislative language in the 1911, 1920 and 1930 Acts is broad, the distinction between espionage and journalism is fundamental and its importance has been articulated many times in Parliament and the courts, as well as by journalists and civil society. We do not consider that the case has been made for amending the espionage-focused offences in the 1911, 1920 and 1930 Acts, particularly given that some of the changes suggested would appear to broaden their scope.

Disclosure of official information

iii. Removing the requirement to prove damage would be a retrograde step that takes us back towards the discredited 1911 Section 2 and its catch-all provisions. In principle, criminal sanction should only be applied to disclosures that can be demonstrated to have the potential to cause serious damage. The requirement to prove damage under the 1989 Act was explicitly stated to have a public interest component.

4 Duncan Campbell, Planned Espionage Act could jail journos and whistleblowers as spies, The Register (10 February 2017). https://www.theregister.co.uk/2017/02/10/espionage_law_jail_journalists_as_spies/

iv. We do not think the case has been made for introducing a new category of protected economic information.

v. The proposed extraterritorial provisions are vague in scope. It is not clear that consideration has been given to whether they would be enforceable in practice.

vi. We do not consider that the case has been made for increasing the penalties for unauthorised disclosure offences.

vii. We see a clear need for a statutory public interest defence. The adoption of a commissioner model is a step forward, but insufficient on its own. We consider that the combination of a commissioner plus statutory public interest defence, as in the Canadian model, represents the optimal solution.

Introduction

Governments have valid interests in keeping some information confidential.[5] In a democracy, there will always be a tension between these interests and those of the general public in being able to hold government to account. The understanding of what information should be public and what should be protected is subject to changing norms.[6]

Criminal sanctions are just one of the methods by which governments manage the release of information, but they are among the most draconian. Britain's Official Secrets legislation has been controversial ever since its first introduction in the late nineteenth century and Parliamentary scrutiny of these provisions has not always been as thorough as it might be. The catch-all prohibition on the release of official information in Section 2 of the 1911 Official Secrets Act reached the statute book without any

5 See, for instance Franks ¶11

6 Moran provides an account of the evolution of central government's relations with the media and an increasing trend towards managed disclosure. Moran, C. Classified: Secrecy and the State in Modern Britain. (2013)

debate at all.[7] The old Section 2 fell into disrepute in the post-war era, although decades passed before it was actually reformed in 1989.[8]

A similar length of time has now passed since the law was last changed in 1989 and the context in which the legislation operates has changed in a number of important respects. Since 2000, the Freedom of Information Act has enabled members of public to request the release of official information, subject to various exemptions and a public interest test. The Public Administration Select Committee has acknowledged that there is a conflict between this public interest standard and that for criminal liability under the Official Secrets Act 1989: information released under FOI rules could become the subject of criminal prosecution if disclosed by a civil servant by other means.[9]

There is also a greater acknowledgement of the importance of whistleblowers and sources, who often put themselves at considerable risk in order to bring information to public attention. Commitments have been made at G20 level to ensure that national laws offer protection to whistleblowers.[10] The UK has its own whistleblower protection law in the form of the 1998 Public Interest Disclosure Act (PIDA). While PIDA does not apply to employees of the security services, there is a growing recognition internationally that whistleblowers whose disclosures concern national security information are also entitled to a degree of protection. The 2013 Global Principles on National Security and the Right to Information (the Tshwane Principles) form the gold standard in this area and have been endorsed by the Council of Europe.[11]

7 Franks ¶ 49

8 In 1972 the Franks Report was unequivocal that the old Section 2 had lost public confidence and was badly in need of reform or repeal. Franks ¶ 8-9 & 14 & 25; David Hooper, Official Secrets: The Use and Abuse of the Act (Secker & Warburg, 1987) pp.228-234 (hereafter Hooper)

9 Public Administration Select Committee (2009). Leaks and Whistleblowing in Whitehall. ¶ 28, 32

10 Blueprint for Free Speech have been monitoring how countries are meeting this commitment. https://blueprintforfreespeech.net/wp-content/uploads/2015/09/Whistleblower-Protection-Laws-in-G20-Countries-Priorities-for-Action.pdf

11 Council of Europe Parliamentary Assembly Resolution 1954 (2013)

The importance of journalism's watchdog function in democratic societies is not in doubt. Changes in the news media and the rise of citizen journalism mean that the distinction between professional journalists and members of the public is no longer as hard as it used to be. Recent years have seen heightened threats to journalists and their sources, even in democratic societies.[12] Surveillance adds an extra dimension to the debate and there are worrying examples of these powers being used to unmask journalists' sources in the UK.[13]

It is unfortunate that these concerns do not come through more clearly in the Law Commission's report. The pre-consultation exercise compares poorly to the range and number of witnesses consulted by the Franks Committee. We think a wider consultation process is necessary before draft legislation is produced.

It is important that the full range of voices are heard in this consultation. We suggest that an interim report and further consultations with civil society, media groups and other interested parties may be useful before draft legislation is produced.

Unauthorised disclosures do of course pose some issues for public authorities. However, set against this is the recognition on both sides of the Atlantic that 'official leaking' - that is, anonymous briefing to journalists - is a routine part of the way government works.[14] Academics have found that unauthorised leaking too plays an important - though not unproblematic - role in ensuring good governance.[15]

12 Information Law and Policy Centre (2016), Protecting Sources and Whistleblowers in a Digital Age, pp.4

13 See, for example, the Investigatory Powers Tribunal's recent ruling against Cleveland Police. [2017] UKIPTrib15_586-CH

14 David E. Pozen, 'The Leaky Leviathan: Why the Government Condemns and Condones Unlawful Disclosures of Information' (2013) 127 Harvard Law Review 512; Lustgarten, L. and Leigh, I., In From the Cold: National Security and Parliamentary Democracy (OUP, 1994); Public Aministration Select Committee ¶ 32, 36

15 Sagar, R. Secrets and Leaks: The Dilemma of State Secrecy (Princeton University Press, 2013); Yochai Benkler, A Public Accountability Defense For National Security Leakers and Whistleblowers, 8 Harv. L. & Pol'y Rev. 281 (2014).

While the case of NSA whistleblower Edward Snowden is not directly addressed in the report, it does appear to underlie many of the report's concerns – about the use of technology to facilitate disclosure, the extraterritorial reach of UK law and whether existing penalties are adequate. By not addressing the Snowden case directly, the report elides the fundamental issue at play: that there may very well be significant public interest in unauthorised disclosures, even sensitive ones.[16]

If the underlying aim of the present exercise is to limit the occurrence of anonymous or bulk leaking of official information, directly addressing the case of Edward Snowden could have provided another important insight: that of the role effective internal reporting channels and statutory public interest defences have in achieving that goal. Though some internal channels for expressing concerns existed in the context Edward Snowden worked in, as an NSA contractor rather than a direct employee he was not entitled to take advantage of them. There were also significant concerns about the effectiveness of those channels in protecting those who made use of them. Edward Snowden has stated that the experience of NSA whistleblower Thomas Drake informed his own decision-making.[17]

Another side of this situation is that governments and public bodies also have a responsibility to protect information. This is a technological issue as well as a legal one. Key examples from the United States illustrate the importance of proper information security practices. The compromise of electronic records held by the Office of Personnel Management - reportedly by China - followed repeated warnings of "persistent weaknesses" in the organisation's information security infrastructure.[18] The House Select Committee on Intelligence's declassified report on Edward Snowden's disclosures concluded that not

16 Edward Snowden's revelations about global surveillance have led to legislative reforms, court cases and changed business practices too numerous to recount here. Of particular relevance in the current context might be the ruling of the Investigatory Powers Tribunal that the UK-US information sharing regime was unlawful during the eight year period where the public was not properly informed about it: https://www.theguardian.com/uk-news/2015/feb/06/gchq-mass-internet-surveillance-unlawful-court-nsa

17 https://theintercept.com/2016/05/23/vindication-for-edward-snowden-from-a-new-player-in-nsa-whistleblowing-saga/

18 David Auerbach (2015), The OPM Breach is a Catastrophe, Slate, http://www.slate.com/articles/technology/future_tense/2015/06/opm_hack_it_s_a_catastrophe_here_s_how_the_government_can_stop_the_next.html

enough had been done to minimise the risk of leaks.[19] An effective approach to the protection of official data requires more than criminal penalties for espionage or disclosure.

19 Review of the Unauthorized Disclosures of Former National Security Agency Contractor Edward Snowden (15 September 2016) http://intelligence.house.gov/uploadedfiles/hpsci_snowden_review_declassified.pdf

The Espionage Clauses (1911, 1920 and 1939 Official Secrets Acts)

The distinction between espionage and journalism is fundamental.[20] Journalistic activity should therefore not be pulled into the ambit of the espionage offences in Section 1 of the 1911 Act.

The Commissioners are nonetheless correct to point out that the wording of the existing offence, which includes "obtaining and gathering" information, is expansive. Not only could the language Section 1 theoretically apply to journalists, there have in fact been attempts to prosecute them in the past. The prosecution argument advanced at the ABC trial in 1978, that there was a point at which legitimate investigative journalism crossed the line into espionage, was nevertheless comprehensively rejected and the charges withdrawn.[21]

Historically, Parliament has attempted to preserve the distinction between legitimate jouranalistic activity and espionagte. The 1939 Act was motivated by the conviction of a journalist for not revealing their source under Section 6 of the 1911 Act and amended the situation so that the provision could only be used in relation to espionage cases. Attorneys General sought to assure Parliament in 1921 and 1949 that the Act was not intended to be used against journalists.[22]

In 1972 the Franks Committee also recognised that there was a sharp distinction between the different offences in the 1911 Act and considered that the inclusion of the old Section 2 offence in the same piece of legislation was in some ways anomalous:

20 See, for example, Lustgarten and Leigh, In From the Cold, pp. 224-6; Franks ¶ 21
21 Geoffrey Robertson, The Justice Game (Vintage, 1999) pp126; Hooper pp117
22 Robertson pp110

"The distinction between espionage and leakage - that is, between those who intend to help an enemy and those who disclose information with no such intent - is important. This distinction should be reflected in the structure of the law."[23]

The Franks Committee considered that the disclosure offences would be better framed in an Official Information Act, to make the distinction clearer to the public.[24]We consider that this proposal still has much to commend it.

Although the legislative language in the 1911, 1920 and 1930 Acts is broad, the distinction between espionage and journalism is fundamental and its importance has been articulated many times in Parliament and the courts, as well as by journalists and civil society.

The Law Commission report provisionally concludes that the language of the Section 1 offences is "archaic" and has the potential to inhibit investigations or prosecutions, but does not offer much in the way of evidence that this is indeed the case. The language in the Act does not appear to have posed problems of interpretation at the ABC Trial in 1978 and the 1989 White Paper stated that "there is no widespread dissatisfaction" with Section 1.[25]

As the Commissioners note, the use of the term "enemy" (as opposed to "foreign power" or an alternative term) did not present an obstacle in the most recent case where it could have been at issue, that of David Houghton.[26] Similarly, the general term "information" - which is proposed as a replacement for the more specific terms like "sketch" and "drawing" is in fact already included in the Act so it is hard to see what the suggested amendment would achieve in practice. It also does not seem to be the case that the language around "prohibited places" is preventing sites like government data

23 Franks ¶ 102
24 Franks ¶ 103
25 Reform of Section 2 of the Official Secrets Act 1911 (June 1989) Cmnd 408 ¶ 2
26 Protection of Official Data ¶ 2.111

centres from being designated as protected locations under the Serious and Organised Crime and Police Act 2005.[27]

Absent any compelling need for revisiting the legislation, some of the proposed amendments could exacerbate existing issues about the potential breadth of the offence. “National security” is arguably a more expansive concept than “defence of the realm.”[28] We have a similar concern about the proposals for defining a “foreign power” along the lines of the Espionage Statutes Modernization Bill, which in effect means adopting the Foreign Intelligence Surveillance Act definition of a foreign power.[29]

Senator Cardin’s 2010 speech introducing the Espionage Statutes Modernization Bill made it clear that it was intended to target unauthorised disclosures from government officials as well as espionage cases.[30] At the time, observers of US national security legislation described the scope of the Bill as "breathtaking."[31]

If the Commission's intention is "not … to expand the scope of the Official Secrets Act 1911" there does not seem to be a compelling reason for redrafting this section of the Act.

We do not consider that the case has been made for amending the Espionage-focused offences in the 1911, 1920 and 1930 Acts, particularly given that some of the changes suggested would appear to broaden their scope.

27 See, for example: https://www.gov.uk/government/ publications/trespass-on-protected-sites-sections-128-131-of-the-serious-organised-crime-and-police-act-2005

28 In From the Cold, pp. 23-26

29 Protection of Official Data ¶ 2.141, 2.144

30 See: Robert Chesney, The Espionage Statutes Modernization Act of 2010, Lawfare: https://lawfareblog.com/espionage-statutes-modification-act-2010

31 See: Emily Peterson, WikiLeaks and the Espionage Act of 1917, Reporters Committee for Freedom of the Press https://www.rcfp.org/browse-media-law-resources/news-media-law/news-media-and-law-summer-2011/wikileaks-and-espionage-act

Disclosure of official information

Removing the damage test

One of the major reasons why the pre-1989 Section 2 fell into such disrepute was the absence of a harm test, which meant that prosecution could result from the disclosure of even quite trivial official information. David Hooper recounts a number of "bewilderingly petty" cases that were prosecuted under the old Section 2.[32]

The Franks Report and subsequent White Papers have all articulated the position that the criminal law should not be used against disclosures that are trivial, or even those that are undesirable or embarrassing to the government, but only in those cases where serious harm would result.[33] A separate issue with the old catch-all offence was that, as Franks noted, ministers and senior civil servants are effectively 'self-authorising', so the law didn't apply to individuals equally.[34] Since the passage of the Freedom of Information Act, public expectations have in any case moved in the direction of greater official openness.

The Law Commission report proposes a replacing the harm test with a subjective one of the defendant's state of mind. We think this is a step backwards and effectively a move towards strict liability as it is difficult to forsee a circumstance in which a defendant could show they had no reason to believe that the information fell within a category protected by the Act, some of which are very broad.

Furthermore, the position articulated in the 1989 White Paper was that the public interest test was encompassed by the need for the prosecution to show that a disclosure was damaging.[35] While we do

32 Hooper, pp. 7
33 Franks ¶ 116-120; White Paper of June 1988 Reform of Section 2 of the Official Secrets Act 1911 (Cmnd 408) at ¶ 14, 24
34 Franks ¶ 18
35 Reform of Section 2 of the Official Secrets Act 1911 (June 1989) Cmnd 408 ¶ 59-61

not think this is a sufficient treatment of the public interest factor – and the Tshwane Principles agree that a damaging disclosure may still nonetheless be in the public interest[36] - removing the harm test would break the explcit compromise reached in the 1989 Act.

Given that the Tshwane Principles also advocate linking classification levels to the potential harm caused by disclosure,[37] we think it is worth revisiting the approach taken by the Franks Committee. Franks recommended the adoption of a two stage test, with only "seriously damaging" disclosures within specified categories carrying the sanction of the criminal law.[38] Furthermore, Franks proposed that classification (at the level of Secret or above) be used as a measure of harm likely to be caused by disclosure.[39]

Subsequent White Papers took issue with the Franks approach largely on the basis of how classification could be demonstrated in court, but did not contest that showing harm, or the potential to cause harm, should form part of the offence. The 1989 White Paper proposed that the harm test should vary by category, with the bar in some categories being very low. Observers of the 1989 Act have stated that it does not represent a high evidential barrier for the prosecution.[40]

The Law Commission report suggests that it is undesirable for defendants to escape prosecution when evidence relating to harm cannot be shown in court, but it is difficult to see why this should ever be the case given that procedures for closed session were provided for in the 1920 Act and were used in at least eight cases before 1989.[41] Of cases brought after 1989, we note that the memo at issue in the *Keogh* case has still not been made public.

36 Tshwane Principles ¶ 43 – damage is one of a number of factors to be used in weighing up whether a disclosure was in the public interest.
37 Tshwane Principles ¶ 11
38 Franks ¶ 54
39 Franks ¶ 144.
40 Savage, A. Leaks, Whistleblowing and the Public Interest. (Edward Elgar, 2016) pp.23, 50; Article 19 and Liberty (2000), Secrets, Spies and Whistleblowers.
41 Hooper, pp 53, 81, 173, 249, 251, 255, 259, 271

Removing the requirement to prove damage would be a retrograde step that takes us back to the discredited 1911 Act and its catch-all provisions. In principle, criminal sanction should only be applied to disclosures that have the potential to cause serious damage. The requirement to prove damage under the 1989 Act was explicitly stated to have a public interest component.

Information relating to the economy

The inclusion of economic matters as a category of protected information was examined by the Franks Committee, with some support for information relating to the reserves and the exchange rate being protected under the Official Secrets Act. As the interest rate regime changed, this position was later revised. In November 1976, Home Secretary Merlyn Rees told Parliament that, as a result, economic matters no longer pertained to international relations, but to domestic politics and there was therefore no longer a reason for them to be protected with criminal sanction. Subsequent White Papers have agreed with that position.[42]

The consultation document asks respondents whether “sensitive information relating to the economy so far as it relates to national security be brought within the scope of the legislation or is such a formulation too narrow?”[43]

This suggestion for a new category of protected information is presented with little in the way of supporting argument or concrete examples. Without these, it is very unclear what "information relating to the economy insofar as it relates to national security" adds which isn't already covered by existing categories, or how the situation has changed since 1989.

42 HC Deb 22 November 1976 vol 919 cc1878-88; Reform of Section 2 of the Official Secrets Act 1911 (January 1978) Cmnd 7285 ¶ 12; Reform of Section 2 of the Official Secrets Act 1911 (June 1989) Cmnd 408 ¶ 33
43 Law Commission, Protection of Official Data ¶ 3.214

Similar concerns about the term were put forward by the Intelligence and Security Committee and the Joint Committee in relation to the Investigatory Powers Act, while it was being scrutinised in Parliament. The Joint Committee recommended that the term be defined in legislation "in order to provide clarity".[44] In their report on the Draft Investigatory Powers Bill, the Intelligence and Security Committee stated:

"if 'national security' is sufficient in itself, then "*economic well-being… so far as [is] relevant to the interests of national security*" is redundant, since it is a subset of the former. We have questioned both the Agencies and the Home Office on this matter and neither have provided any sensible explanation. In our opinion, this area is already sufficiently complex so drafters should seek to minimise confusion wherever possible. We therefore recommend that 'economic well-being' is removed as a separate category."[45]

It is important to remember that the inclusion of "information relating to the economy insofar as it relates to national security" in the Investigatory Powers Act is as a ground for surveillance warrants. Given that procedures for the gathering of intelligence are generally subject to a lower legal threshold than those which normally govern the gathering of evidence for use in criminal proceedings, we do not think it is appropriate to transplant this category directly into the criminal law.[46]

We do not think the case has been made for introducing a new category of protected economic information.

Extraterritorial clauses

44 Joint Committee on the Draft Investigatory Powers Bill, Report (11 February 2016) ¶ 696
45 Intelligence and Security Committee, Report on the Draft Investigatory Powers Bill (9 Feburary 2016), HC795, pp.10
46 UN Doc A/HRC/16/50 ¶ 40

New extraterritorial provisions would appear to significantly broaden the scope of the offences from British officers and subjects to those with a "significant link" to the UK.[47] The Report refers to the 2015 amendments of the Computer Misuse Act, which uses the same term "applied in various ways". It is unclear what a "significant link" might mean in practice and whether the Commission is proposing that foreign journalists, for instance, might face prosecution if they published information that falls into a category protected by the Official Secrets Act.

If this is indeed what the Commission is proposing, it is unclear whether thought has been given to the likely possibility of foreign nationals being extradited to face charges of this type in the UK, particularly given the French courts' refusal to extradite David Shayler in 1998.[48]

Not only does it undermine the principle of deterrence if laws are unenforcable, the assertion of extraterrorial jurisdiction raises the possibility of states trying to enforce reciprocal laws against UK citizens.

The proposed extraterritorial provisions are vague in scope. It is not clear that consideration has been given to whether they would be enforceable in practice.

Sentencing

While we recognise that the Law Commission is not suggesting that the maximum sentence for the disclosure offences should be raised from 2 to 14 years, we do not see the case has been made for increased penalties. The history of prosecutions under the 1989 Act does not, to the best of our knowledge, reveal an example of someone being sentenced to the maximum 2 years, still less an instance where the maximum sentence has been stated to be inadequate.

47 Protection of Official Data, 2.175
48 Savage, pp.73

While the Franks Committee looked closely at the penalties available under the existing legislation in 1972, they saw no reason to increase custodial sentences. As those working in the field have noted, in practice the penalties whistleblowers face for acting are often very severe – including employer retaliation, loss of income and livelihood – even if they are not prosecuted.

We do not consider that the case has been made for increasing the penalties for unauthorised disclosure offences.

Public interest defence

There have been calls for a public interest defence to the Official Secrets Act ever since it was first introduced. The current protections for defendants who would wish to argue that they acted in the public interest are very weak. The common law defence of necessity has not been tested since the *Shayler* case, although it is reported that GCHQ translator Katherine Gunn would have tried to raise this defence had the case against her not collapsed. Historically, juries have sometimes returned perverse verdicts in cases where matters of public interest are at play and notably did so in the case of Clive Ponting.[49] In practice, considerations of public interest – or how controversial a case is likely to be – likely also play a role in the Attorney General's decision to pursue a prosecution.[50]

The Law Commission report notes that the only test to date of whether the 1989 Act is compatible with Article 10 of the European Convention on Human Rights was conducted by the House of Lords in the *Shayler* case in 2002. It further argues that recent case law of the Strasbourg court – the *Guja v Moldova* and *Bucur v Romania* rulings in particular – supports the introduction of internal reporting channels but does not require that a public interest defence be available.[51] Other analysts disagree with this analysis

49 EP Thomson, Writing by Candlelight (Merlin Press, 1980), pp.99-111; Hooper pp.139-160
50 Savage, p67
51 Protection of Official Data ¶ 6.76

and think it is “increasingly likely” that the absence of a statutory public interest defence renders the 1989 Act incompatible with Article 10.[52]

The Law Commission’s Information for Consultees does acknowledge that the Grand Chamber of ECtHR has held that public disclosure of information should be available as a last resort. The Tshwane Principles also support the introduction of a public interest defence to be used as a last resort, regardless if internal channels have been used first, to weigh “if the public interest in disclosure of the information in question outweighs the public harm in non-disclosure”.[53]

In their information for Consultees, the Commissioners provide a four point summary of their arguments against a statutory public interest defence.[54] Firstly, it is claimed that a public interest defence "erodes the impartiality of the civil service by permitting civil servants to weigh government policy against other values." In fact, as noted by the Public Administration Committee, civil servants already have obligations “to weigh government policy against other values”, for instance in their duty to ensure that Parliament is not misled.[55] The Committee found that, “as a last resort”, a civil servant might be entitled to report concerns outside the civil service, for instance to the head of the relevant Select Committee.

Secondly, it is argued that a public interest defence would erode public trust in the intelligence services in particular. This neglects the extent to which ensuring that the public is properly informed is also critical to trust and reputation. This requirement for trust running in both directions was one of the issues at the centre of David Anderson’s review of investigatory powers *A Question of Trust*, which was prepared in the aftermath of Edward Snowden’s revelations.[56] As previously mentioned, the Investigatory Powers Tribunal has ruled that some of GCHQ’s practice was unlawful while it was concealed from the public.

52 Savage, pp70
53 Tshwane Principles ¶ 38-41, 43
54 Information for Consultees ¶ 1.19
55 Public Administration Committee ¶ 26
56 David Anderson, A Question of Trust, 3.12-3.13

The third contention offered about the introduction of a statutory public interest defence is that it would encourage reckless disclosure. The evidence is not on the side of whistleblowers acting recklessly where protections are available to them, such as those offered under the Public Interest Disclosure Act. Public Concern at Work's 2013 report *Whistleblowing: The Inside Story*, based on the experience of 1000 whistleblowers who used the organisation's advice line, showed that whistleblowers are overwhelmingly likely to attempt to report their concerns internally and typically try to do so a number of times. The report also found that whistleblowers act with a strong awareness of the negative consequences they may face personally as a result.[57]

The fourth and final argument offered against the introduction of a a statutory public interest defence is that it would create legal uncertainty. Courts and Juries can and do contend with the concept of the public interest in other situations. Cases involving the law of confidence, data protection or the Public Interest Disclosure Act will often involve individuals having to make this kind of judgement. It is not obvious why cases involving the disclosure of official information should be considered differently.

There's also already a degree of uncertainty in Official Secrets Act cases as the Attorney General makes the decision about whether to prosecute. Furthermore, in at least three cases brought under the 1989 Act – that of Katherine Gunn, Derek Pasquill and the second against Richard Tomlinson – charges have either been dropped or the prosecution has declined to offer evidence. In other words, this is a system in which public interest factors play a role and do so in a very unpredictable manner. A statutory public interest defence would likely make the system more predictable, rather than less.

We see a clear need for a statutory public interest defence.

57 Public Concern at Work (2013), Whistleblowing: the Inside Story http://www.pcaw.org.uk/files/Whistleblowing%20-%20the%20inside%20story%20FINAL.pdf

This is not to say that a statutory public interest defence should stand alone. We agree that defined routes of access to independent oversight bodies are essential. Nevertheless, as seen in the case of *Bucur v Romania*, oversight bodies can be ineffective or the creature of the institutions they are meant to oversee. It is recognised in the Law Commission report that the internal channel David Shayler was told he should make use of – the staff counsellor – does in fact need supplementing with a more formal independent commissioner system.[58] The case of NSA whistleblower Thomas Drake, who faced retaliation for making use of the internal channels open to him, provides a salutary example of how things can go wrong.[59]

We think that the best way of ensuring that the commissioner system is effective is to introduce the entire Canadian model - that is, ensure that a public interest defence is available as a backstop. This is essentially also the model recommended in the Tshwane Principles. It is not clear why the law Commission conclude that the fact that the Canadian public interest defence has not been invoked in court means that it is ineffective: it could equally mean that it has achieved its purpose in ensuring that concerns are dealt with by the commissioner.

The report suggests that the recently-appointed Investigatory Powers Commissioner be made responsible for dealing with concerns from security and intelligence services employees. Given that the Investigatory Powers Act makes provisions for reporting concerns about the exercise of those powers to the commissioner, this seems appropriate as long as the Commissioner's workload is manageable. We note that one of the bodies whose role has been subsumed into the new Commissioner's office sounded a warning in this regard.[60]

58 Protection of Official Data ¶ 7.116
59 https://www.theguardian.com/us-news/2016/may/22/how-pentagon-punished-nsa-whistleblowers
60 See the IOCCO submission to the Joint Committee scrutinising the Investigatory Powers Bill: http://www.iocco-uk.info/docs/IOCCO%20Evidence%20for%20the%20IP%20Bill%20Joint%20Committee.pdf

Finally, given that the Intelligence and Security Committee is also responsible for oversight of the security and intelligence services, we think consideration should be given as to whether individuals should be empowered to report their concerns to the Committee, either directly or via the Commissioner.

The adoption of a commissioner model is a step forward, but not sufficient on its own. We consider that the combination of a commissioner plus statutory public interest defence, as in the Canadian model, represents the optimal solution.