Solicitors & Attorneys

Criminal Law Team
Law Commission
1st Floor Tower
52 Queen Anne's Gate
London SW1H 9AG

By email: pod@lawcommission.gsi.gov.uk

3 May 2017

Dear Sirs,

Re: Response to Consultation on Protection of Official Data

A. Overview

This is an area of law where the same issue arises repeatedly. The law falls into disrepute and then disuse due to its overbroad reach – having rendered itself and the prosecuting State ridiculous --harming the rule of law. Lessons must be learned from the past. All involved should actually read the seminal Frank's Report (Franks). The consultation paper is admirable but no match for Franks. Further, it would undo Franks and roll back to a 1911 approach. Indeed, the tabled reforms feature three elements: a catch all criminal offence, limited by the dispensation of authorization and the Attorney-General's consent to prosecute. But Franks recommended the repeal of the 61 year old Act's §.2 (of 1911) and its "catch all" criminal offence of unauthorized[1] disclosure applicable to *all official information and documents*[2] and *all* Crown Servants,[3] —"*saved from absurdity*" only by the Attorney-General's sparing consent to prosecute.[4] Then as now, the only limit was authorisation.

B. Key lessons from the past

We think the key elements of Franks that should inform change now are:

1. Only truly secret information should be protected by the sanction of criminal law. No offence should catch all official data.
2. The information must have been classified as secret and protected

[1]See Franks ¶ 31-33 (including self and implicit authorisations).
[2]See Franks ¶ 89 "*it deals with information of all kinds and it catches people who have no thought of harming their country. Many consider it wrong that such a provision should appear side by side with the rest [of the Act]*".
[3]See Franks ¶ 17.
[4]It had therefore fallen into disrepute and the public has lost confidence in it—in part due to the acquittals of the Telegraph and its editor and sources in the Nigerian case—and the need for reform had become a cause celebre. See Franks ¶ 8-9 & 14 & 25.

as such. Resources can be better allocated to protecting the smallest possible class of truly secret data.

3. The criminal law should not apply even where there may be *some* injury from a leak. A *serious* injury standard should be retained as an additional safeguard against overreach together with Attorney-General's consent and certificate.
4. Other confidential information –if leaked –may be dealt with by civil law and other sanctions.
5. Mere receipt and other conduct by citizens and publication by the media should not be criminalised.

The White papers of 1978 and 1988 complete the picture as they demonstrate that what is regarded as deserving of protection and what should be published/released are the subject of changing fashions and norms. This suggests that tests and thresholds with proper flexibility such as the serious injury test should be kept. New norms applicable today include our general default rule of freedom of official information, and, under the ECHR and its jurisprudence, the fact that derogations from convention rights must be prescribed by law and foreseeable so the citizen can know what the law is and adapt his conduct. As applied even in the context of security and intelligence surveillance, the surveillance regimes and systems that impact citizens must be made public. Further, in the modern media age, when the media is no longer just professionals but includes the citizen journalist, a proper defence with knowable contours and reasonable predictability is required.

C. Franks

The key recommendations were:

1. The Act should be limited to spying and related matters and renamed the Espionage Act. There should be a new *Official Information Act*[5] –with the objective of bringing more information into the public domain to reflect the new policy of open government[6]—and to free resources for protecting what was *genuinely secret.*[7]
2. In balancing secrecy and openness --the criminal law should only be engaged to guard against disclosures *seriously damaging the*

[5]See Franks ¶103.
[6]Arising out of the Fulton Committee (on the Civil Service) Report of 1968 and its concern with "too much secrecy" and the 1969 White Paper on Information and the Public Interest. See Franks ¶ 5.
[7]See Franks ¶ 67 and 107 and 110.

security of the nation and the safety of the people.[8] It should not apply to mere leakage (with no such intent)[9] and leaks that were *merely embarrassing* for the government of the day had to be tolerated. [10]

3. Disclosure of much information by Crown Servants would be decriminalized. Constraints remained such as career progression, disciplinary action and dismissal.[11]
4. The replacement offence would be much narrower covering *three main categories only*; (1) National Security/Defence;[12](2) foreign relations (not affairs); and (3) currency and reserves. Apart from Cabinet documents and personal data of citizens', disclosure of all other data was to fall outside the scope of the criminal law.[13]
5. Even within National Security/Defence only the following were deserving of protection: (a) the Armed Forces; (b) military weapons and equipment and communications; (c) research and development of the same; (d) defence policy, strategy and military planning for war, (e) intelligence and security services and information obtained by them; (f) military treaties and arrangements with other nations and negotiations for them, and (g) homeland defence and security in the event of war.[14] Similar information from allies would be protected.
6. A new second element to the new offence, a damage based test of "*serious injury to the nation*" –would narrow the information caught by the criminal law.[15] The criminal law was not to apply to unauthorized disclosures falling short of this standard and

[8]See Franks ¶ 54.
[9]See Franks ¶ 102.
[10]See The Home Secretary's statement of 22 November 1976, Official Report, col 1879, cited in The White Paper of July 1978 (Reform of Section 2 of the Official Secrets Act 1911 (January 1978) Cmnd 7285) and see the Reform of Section 2 of the Official Secrets Act 1911 herein White Paper of June 1988 (Cmnd 408) at ¶14 "*..it is not sufficient [to engage the criminal law] that the disclosure is undesirable, a betrayal of trust or an embarrassment to the Government"* and at ¶24 "*..even if disclosure may obstruct sensible and equitable administration, cause local damage to individuals or groups or result in political embarrassment, it does not impinge on any wider public interest to a degree which would justify applying criminal sanctions."*
[11]See Franks ¶ 58-59.
[12]See Franks ¶ 124-5, where the information protected would be similar to that covered by the D Notice system.
[13]See Franks ¶ 120-143.
[14]See Franks ¶ 124.
[15]See Franks ¶ 117-119.

causing *some* injury—*even within the three categories defined.* [16]

7. In order to be protected, written information even within the three categories had to be *classified and labelled and marked* as top secret, secret or defence-confidential (adapting existing standards).[17] Much orally imparted information would be in a classified document somewhere and so also covered.[18] It was the Government's duty to identify such material and classify it.[19] These *security classifications:* top secret/secret, defence-confidential respectively mapped over to/were applied in the first place where the grave/damage/prejudice to the safety or interests of the nation standards applied. [20] That is, disclosure of the information would have to be seriously damaging *in order for the information to warrant the marking and protection in the first place.*

8. So the new offence would be two limbed: (1) the information was within the three categories; and (2) it was marked as classified --on the grounds that its unauthorized disclosure would cause *a serious injury to the interests of the nation.*[21]

9. It was not to be left to the courts to decide whether a disclosure had seriously harmed the nation, as juries lacked the experience and the issues were for the executive (and due to difficulties with secret evidence and the right to a fair trial). In a prosecution scenario, the Minister was to certify that the classification was properly applied and correct—and this would operate as an additional safeguard against over-classification.

10. Due to suspicions about over-classification to prevent disclosure of matters of public interest, a committee should be formed of government and media to help third parties in possession of Official Information and to help the government classify.

11. Other protected areas were: (a) the three heads of law and order information (information likely to be helpful in the commission of an offence or an escape or impede detection or prevention of offences) and (b) what today would be called personal data (confidences of the citizen reposed in government) and (c) Cabinet papers necessary to protect collective responsibility and (d) commercial data arising from dealings with

[16]See Franks ¶ 118 & 120. This appears to be have been misunderstood in the June 1988 White Paper at **¶9**.
[17]See Franks ¶ 148-149.
[18]See Franks ¶ 152.
[19]See Franks ¶ 144 & 145-146.
[20]See Franks ¶ 61-64 and 151.
[21]See Franks ¶ 149 & 157.

the public sector.

12. The act should impose on Crown Servants a duty to protect Official Information. That class included Ministers, members of the Home and Diplomatic service, armed forces, police forces, post office and persons working for the same and former members of such a class. It should be an offence for these Crown Servants to communicate information to which the act applied, contrary to his official duty.[22] Many disclosures were authorized or self authorized or made in the course of duties.[23] Those entrusted with official information in confidence (such as contractors) should also be treated comparably.

13. A mens rea requirement had to be clear. §2 was not. The new standard was to be reasonable grounds for knowledge or belief or knowledge that he had acted contrary to his duty.[24] Failure to take reasonable care would also be an offence. Lack of knowledge that the information was classified would be a defence (note how this is relevant to classification).

14. The criminalization of the *mere receipt* of official information by a citizen in §2(2) should be abolished.[25] Other laws (such as on corruption) tended to the gap. In relation to the personal data head, once leaked it could be difficult for a citizen to track and recognize and so dealings should not be criminal. As for the rest, the public as subjects of the Crown, had a duty to protect Official Information, but an individual should not face a conviction for an unauthorized communication unless he had mens rea (or knew or had reasonable grounds to believe the information had come to him as a result of a contravention of law by a Crown Servant, contractor or confidee of the same). The prosecution should have to prove against a citizen: (a) a contravention of the act by some person; and (b) that the information was still covered by the act when the accused communicated it; and (c) that the accused knew that the information had at some earlier stage been communicated in contravention of the act or had reasonable grounds to believe this was the case. It should be a defence that the accused believed reasonably that an authorization applied and communication for obtaining an authorization should not be an offence.[26] It should be a defence that it had come into his hands innocently and he did not know and had no reason to believe that disclosure of the document might cause serious injury to the

[22]See Franks ¶ 215-217.
[23]See Franks ¶ 18-33.
[24]See Franks ¶ 152 & 218-222.
[25]See Franks ¶ 19 and (e) & 232-3.
[26]See Franks ¶ 234-236.

interests of the nation and no offence should be committed unless it is proved the document was marked secret. [27]

15. While only two post war cases prosecuted professional journalists, it had a strong chilling effect on speech and threats were often made to the media by the civil service.[28] It was noted that the unauthorized disclosure of Official Information did not have the effect of bringing it in to the public domain[29].

16. The Act would apply to the Official Information of allies coming into the hands of Crown Servants in the same way as to domestic Official Information. [30]

17. Work was to commence on a study on the desirability of FOIA *and broadly speaking this would cover what was not protected* by the Official Information Act. [31]

D. The White Papers of 1978 and 1988

The White Paper of July 1978[32] concurred with Franks but suggested some changes. These include that the Minister's certification on classification be bolstered by the Attorney-General's endorsement on the classification.[33] Wider protection for economic information was recommended but less for Cabinet documents. A new general protected category was added for "intelligence and security."[34] It was recommended that all of this information should be protected whether or not it was classified, due to the risk of aggregation. In foreign relations –the line was to be drawn at a test of "prejudicial to the nation" or the "Confidential" classification. Franks had recommended that "Defence-Confidential" be used only for information on military weapons and equipment but it was recommended this extend to defence policy and strategy, intelligence and security and military treaties and arrangements and internal defence and security. Criminal sanctions would only be appropriate for some of the additional information—adopting the prejudicial test would catch a considerable body of information but the Government agreed with the Franks Test of serious

[27]See Franks ¶ 237.
[28]See Franks ¶ 25 & 26 -29.
[29]See Franks ¶ 229.
[30]See Franks ¶ 263 .
[31]See Franks ¶ 87.
[32]Reform of Section 2 of the Official Secrets Act 1911 (January 1978) Cmnd 7285
[33]Reform of Section 2 of the Official Secrets Act 1911 (January 1978) Cmnd 7285 ¶11.
[34]Reform of Section 2 of the Official Secrets Act 1911 (January 1978) Cmnd 7285 ¶15.

injury. Failure to mark should not be determinative of liability – which should be left to the serious injury test. In relation to law and order –the criminal sanction had to be limited to when strong reasons applied. In relation to a disclosure by a citizen, the predicate breach by another should be removed and the knowledge or reasonable cause to believe that the information was protected standard should alone apply (otherwise if given by a Crown Servant, the sanction would apply-- but not if the citizen had stolen it).

The June 1988 White Paper[35] noted that while prosecutions were not bought for the harmless disclosure of information, it was wrong in principle that the criminal law should extend to them[36] and the section had long been criticized and regarded as an "*oppressive instrument for the suppression of harmless and legitimate discussion*"[37] and this hampered its necessary role. The focus had to be to determine in what circumstances the unauthorized disclosure of information should be criminal. It noted "*..it is not sufficient that the disclosure is undesirable, a betrayal of trust or an embarrassment to the Government*"[38] and "*..even if disclosure may obstruct sensible and equitable administration, cause local damage to individuals or groups or result in political embarrassment, it does not impinge on any wider public interest to a degree which would justify applying criminal sanctions.*"[39] It proposed to replace the Minister's certificate with the finding of a court as it was not acceptable that an element of the offence –the serious harm to the nation --could not be challenged in court.[40] Classification was abandoned and separate and more specific tests of harm introduced for each offence. It went through and made recommendations on each category but mainly kept them.[41] On interception, details of the practices had to be kept secret to remain effective as well as their fruits.[42] Cabinet papers and economic

[35]White Paper of June 1988 Reform of Section 2 of the Official Secrets Act 1911 (Cmnd 408).
[36]White Paper of June 1988 Reform of Section 2 of the Official Secrets Act 1911 (Cmnd 408) at ¶8.
[37]White Paper of June 1988 Reform of Section 2 of the Official Secrets Act 1911 (Cmnd 408) at ¶8.
[38]White Paper of June 1988 Reform of Section 2 of the Official Secrets Act 1911 (Cmnd 408) at ¶14.
[39]White Paper of June 1988 Reform of Section 2 of the Official Secrets Act 1911 (Cmnd 408) at ¶24.
[40]White Paper of June 1988 Reform of Section 2 of the Official Secrets Act 1911 (Cmnd 408) at ¶18.
[41]White Paper of June 1988 Reform of Section 2 of the Official Secrets Act 1911 (Cmnd 408) at ¶31.
[42]White Paper of June 1988 Reform of Section 2 of the Official Secrets Act 1911 (Cmnd 408) at ¶30.

information were now regarded as less deserving of protection.[43] Nor would all disclosures of security and intelligence information be protected—only those that would damage their operation.[44]

As noted, what each of the above papers regarded as deserving of protection and what should be published/released were the subject of changing norms. This suggests that tests and thresholds with flexibility are desirable –such as the serious harm test.

E. FOIA

In 2000, the Freedom of Information Act (FOIA) was passed. Notably the security and intelligence agencies are exempt from the FOIA disclosure regime and from any obligation to confirm possession, see §23. There are also various qualified exemptions where information may be exempt if the public interest in withholding is greater than in disclosure. Factors relevant to this test include promoting transparency, accountability and participation and the quality of the same. This applies to §24 covering information likely to prejudice national security and §27 on information likely to prejudice international relations. Law enforcement information is exempt under §31 if its disclosure would be likely to prejudice the prevention or detection of crime, the apprehension or prosecution of offenders or the administration of justice. By §35 information related to the formulation or development of government policy may be exempt –again if the public interest in withholding is greater than in disclosure. Note that the First Tier Tribunal has disapproved some attempts to withhold on the basis that forced disclosure acts as a check on voluntary disclosure. The case law under the FOIA should inform the Law Commission's exercise. The FOIA reflected the UK's very late adoption of widely accepted international norms about the public domain and the public's need to be informed in a functioning democracy. See also the Council of Europe Convention on Access to Official Documents.

As noted, the ECHR and the growing body of jurisprudence from a series of cases have now made clear that derogations from convention rights must be prescribed by law, foreseeable and proportionate and that means the citizen must be able to know what the law is. In the context of security and intelligence--even surveillance--it is now established that the systems in place that impact citizens must be made public. See *Liberty v Secretary of State for Foreign and Commonwealth Affairs* [2014] UKIPTrib 13_77-H *("the expression "in accordance with the law" within the meaning of Article 8(2) requires, firstly, that the*

[43]White Paper of June 1988 Reform of Section 2 of the Official Secrets Act 1911 (Cmnd 408) at ¶32 & 33.
[44]White Paper of June 1988 Reform of Section 2 of the Official Secrets Act 1911 (Cmnd 408) at ¶38.

impugned measure should have some basis in domestic law; it also refers to the quality of the law in question, requiring that it should be accessible to the person concerned, who must, moreover be able to foresee its consequences for him, and compatible with the rule of law".... the following propositions, which have become known as the *Weber* requirements [from *Weber and Saravia v Germany [2008] 46 EHRR SE5*] ...numbered ..1-6 for convenience. "95. *In its case-law on secret measures of surveillance, the Court has developed the following minimum safeguards that should be set out in statute law in order to avoid abuses of power: (1) the nature of the offences which may give rise to an interception order; (2) a definition of the categories of people liable to have their telephones tapped; (3) a limit on the duration of telephone tapping; (4) the procedure to be followed for examining, using and storing the data obtained; (5) the precautions to be taken when communicating the data to other parties; and (6) the circumstances in which recordings may or must be erased or the tapes destroyed.*" 37. "The relevant principles appear to us to be that in order for interference with Article 8 to be in *accordance with the law*: i) there must not be an unfettered discretion for executive action. There must be controls on the arbitrariness of that action. ii) the nature of the rules must be clear and the ambit of them must be in the public domain so far as possible, an "*adequate indication*" given (*Malone v UK* [1985] 7 EHRR 14 at paragraph 67), so that the existence of interference with privacy may in general terms be foreseeable. [45]

[45]A clear reiteration of these principles is contained in the judgment of the Court in *Bykov v Russia* 4378/02 21 January 2009... It is quite plain, as we have said at paragraph 6 above, that in the field of national security much less is required to be put in the public domain, and the degree of foreseeability must be reduced, because otherwise the whole purpose of the steps taken to protect national security would be at risk. The views of the Court to that effect in paragraphs 67 and 68 of *Malone* are encapsulated by the Court in *Leander v Sweden* [1987] 9 EHRR 433 at paragraph 51: "*However, the requirement of foreseeability in the special context of secret controls of staff in sectors affecting national security cannot be the same as in many other fields. Thus, it cannot mean that an individual should be enabled to foresee precisely what checks will be made in his regard by the Swedish special police service in its efforts to protect national security. Nevertheless, in a system applicable to citizens generally, as under the Personnel Control Ordinance, the law has to be sufficiently clear in its terms to give them an adequate indication as to the circumstances in which and the conditions on which the public authorities are empowered to resort to this kind of secret and potentially dangerous interference with private life. In assessing whether the criterion of foreseeability is satisfied, account may be taken also of instructions or administrative practices which do not have the status of substantive law, in so far as those concerned are made sufficiently aware of their contents. In addition, where the implementation*

See also *Rotaru v Romania* (App. 28341/95) 4 May 2000 (same).

F. Other Models

The Canadian model is recommended in the Law Commission report. However apparently this has not been put to use in practice and that, prima facie, is a complete answer to why it is not fit for purpose. The commissioner model is better than the status quo but there is a risk of deference and capture and it is no substitute for the role of the media as the watchdog of democracy. The Tshwane model is the gold standard. The credentials of this model speak for themselves. Categories of information whose withholding may be necessary to protect a legitimate national security interest are set forth in Principle 9. Like Franks, the drafters also see classification as inherently linked to other issues and as applying a necessary discipline to protection. A list of classified information is recommended and time limits. See Principles 15 & 16 respectively. Principle 17 deals with declassification procedures which are recommended –including a procedure for bulk declassification.

Principle 14 provides:

"Duty to State Reasons for Classifying Information

(a) Whether or not a state has a formal classification process, public authorities are obliged to state reasons for classifying information.

Note: "Classification" is the process by which records that contain sensitive information are reviewed and given a mark to indicate who may have access and how the record is to be handled. It is good practice to institute a formal system of classification, in order to reduce arbitrariness and excessive withholding.

(b) The reasons should indicate the narrow category of information, corresponding to one of the categories listed in Principle 9, to which the information belongs, and describe the harm that could result from disclosure, including its level of seriousness and degree of likelihood.

---

of the law consists of secret measures, not open to scrutiny by the individuals concerned or by the public at large, the law itself, as opposed to the accompanying administrative practice, must indicate the scope of any discretion conferred on the competent authority with sufficient clarity, having regard to the legitimate aim of the measure in question, to give the individual adequate protection against arbitrary interference." 39. We consequently bear carefully in mind the requirement to give adequate protection against arbitrary interference on the one hand, but on the other hand that foreseeability does not require all the rules which govern or exclude that arbitrariness to be disclosed, particularly in the field of national security."

(c) Classification levels, if used, should correspond to the levels and likelihood of harm identified in the justification.

(d) When information is classified, (i) a protective marking should be affixed to the record indicating the level, if any, and maximum duration of classification, and (ii) a statement should be included justifying the need to classify at that level and for that period.

Note: Providing a statement justifying each classification decision is encouraged because it makes officials pay attention to the specific harm that would result from disclosure, and because it facilitates the process of declassification and disclosure. Paragraph-by-paragraph marking further facilitates consistency in disclosure of unclassified portions of documents.

At page 12 it notes:

"A national security interest is not legitimate if its real purpose or primary impact is to protect an interest unrelated to national security, such as protection of government or officials from embarrassment or exposure of wrongdoing; concealment of information about human rights violations, any other violation of law, or the functioning of public institutions; strengthening or perpetuating a particular political interest, party, or ideology; or suppression of lawful protests."

Note also Principle 9:

"(a) Public authorities may restrict the public's right of access to information on national security grounds, but only if such restrictions comply with all of the other provisions of these Principles, the information is held by a public authority, and the information falls within one of the following categories:

(i) Information about on-going defense plans, operations, and capabilities for the length of time that the information is of operational utility.

Note: The phrase "for the length of time that the information is of operational utility" is meant to require disclosure of information once the information no longer reveals anything that could be used by enemies to understand the state's readiness, capacity, or plans.

(ii) Information about the production, capabilities, or use of weapons systems and other military systems, including communications systems.

Note: Such information includes technological data and inventions, and information about production, capabilities, or use. Information about budget lines concerning weapons and other military systems should be

made available to the public. See Principles 10C(3) & 10F. It is good practice for states to maintain and publish a control list of weapons, as encouraged by the Arms Trade Treaty as to conventional weapons. It is also good practice to publish information about weapons, equipment, and troop numbers.

(iii) Information about specific measures to safeguard the territory of the state, critical infrastructure, or critical national institutions (institutions essentielles) against threats or use of force or sabotage, the effectiveness of which depend upon secrecy;

Note: "Critical infrastructure" refers to strategic resources, assets, and systems,whether physical or virtual, so vital to the state that destruction or incapacity of such resources, assets, or systems would have a debilitating impact on national security.

(iv)Information pertaining to, or derived from, the operations, sources, and methods of intelligence services, insofar as they concern national security matters; and

(v) Information concerning national security matters that was supplied by a foreign state or inter-governmental body with an express expectation of confidentiality; and other diplomatic communications insofar as they concern national security matters.

Note: It is good practice for such expectations to be recorded in writing.

Note: To the extent that particular information concerning terrorism, and counter-terrorism measures, is covered by one of the above categories, the public's right of access to such information may be subject to restrictions on national security grounds in accordance with this and other provisions of the Principles. At the same time, some information concerning terrorism or counterterrorism measures may be of particularly high public interest: see e.g., Principles 10A, 10B, and 10H(1).

(b) It is good practice for national law to set forth an exclusive list of categories of information that are at least as narrowly drawn as the above categories.

(c) A state may add a category of information to the above list of categories, but only if the category is specifically identified and narrowly defined and preservation of the information's secrecy is necessary to protect a legitimate national security interest that is set forth in law, as suggested in Principle 2(c). In proposing the category, the state should explain how disclosure of information in the category would harm national security."

Principle 10 contains a list of matters that should be presumptively disclosed. These include information about human rights violations and safeguards against the same and the following categories:

"C. Structures and Powers of Government

Information covered by this Principle includes, without limitation, the following:

(1) The existence of all military, police, security, and intelligence authorities, and subunits.

(2) The laws and regulations applicable to those authorities and their oversight bodies and internal accountability mechanisms, and the names of the officials who head such authorities.

(3) Information needed for evaluating and controlling the expenditure of public funds, including the gross overall budgets, major line items, and basic expenditure information for such authorities.

(4) The existence and terms of concluded bilateral and multilateral agreements, and other major international commitments by the state on national security matters.

D. Decisions to Use Military Force or Acquire Weapons of Mass Destruction

(1) Information covered by this Principle includes information relevant to a decision to commit combat troops or take other military action, including confirmation of the fact of taking such action, its general size and scope, and an explanation of the rationale for it, as well as any information that demonstrates that a fact stated as part of the public rationale was mistaken.

Note: The reference to an action's "general" size and scope recognizes that it should generally be possible to satisfy the high public interest in having access to information relevant to the decision to commit combat troops without revealing all of the details of the operational aspects of the military action in question (see Principle 9).

(2) The possession or acquisition of nuclear weapons, or other weapons of mass destruction, by a state, albeit not necessarily details about their manufacture or operational capabilities, is a matter of overriding public interest and should not be kept secret.

Note: This sub-principle should not be read to endorse, in any way, the acquisition of such weapons.

E. Surveillance

(1) The 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.

Note: This information includes: (a) the laws governing all forms of surveillance, both covert and overt, including indirect surveillance such as profiling and data-mining, and the types of surveillance measures that may be used; (b) the permissible objectives of surveillance;

(c) the threshold of suspicion required to initiate or continue surveillance; (d) limitations on the duration of surveillance measures; (e) procedures for authorizing and reviewing the use of such measures; (f) the types of personal data that may be collected and/or processed for national security purposes; and (g) the criteria that apply to the use, retention, deletion, and transfer of these data.

(2) The public should also have access to information about entities authorized to conduct surveillance, and statistics about the use of such surveillance.

Note: This information includes the identity of each government entity granted specific authorization to conduct particular surveillance each year; the number of surveillance authorizations granted each year to each such entity; the best information available concerning the number of individuals and the number of communications subject to surveillance each year; and whether any surveillance was conducted without specific authorization and if so, by which government entity. The right of the public to be informed does not necessarily extend to the fact, or operational details, of surveillance conducted pursuant to law and consistent with human rights obligations. Such information may be withheld from the public and those subject to surveillance at least until the period of surveillance has been concluded.

(3) In addition, the public should be fully informed of the fact of any illegal surveillance.

Information about such surveillance should be disclosed to the maximum extent without violating the privacy rights of those who were subject to surveillance.

(4) These Principles address the right of the public to access information and are without prejudice to the additional substantive and procedural rights of individuals who have been, or believe that they may have been, subject to surveillance.

Note: It is good practice for public authorities to be required to notify persons who have been subjected to covert surveillance (providing, at a minimum, information on the type of measure that was used, the dates, and the body responsible for authorizing the surveillance measure) insofar as this can be done without jeopardizing on-going operations or sources and methods.

(5) The high presumptions in favor of disclosure recognized by this Principle do not apply in respect of information that relates solely to surveillance of the activities of foreign governments.

Note: Information obtained through covert surveillance, including of the activities of foreign governments, should be subject to disclosure in the circumstances identified in Principle 10A.

F. Financial Information

Information covered by this Principle includes information sufficient to enable the public to understand security sector finances, as well as the rules that govern security sector finances. Such information should include but is not limited to:

(1) Departmental and agency budgets with headline items;

(2) End-of-year financial statements with headline items;

(3) Financial management rules and control mechanisms;

(4) Procurement rules; and

(5) Reports made by supreme audit institutions and other bodies responsible for reviewing financial aspects of the security sector, including summaries of any sections of such reports that are classified.

G. Accountability Concerning Constitutional and Statutory Violations and Other Abuses of Power

This Principle includes information concerning the existence, character, and scale of constitutional or statutory violations and other abuses of power by public authorities or personnel.

H. Public Health, Public Safety, or the Environment

Information covered by this Principle includes:

(1) In the event of any imminent or actual threat to public health, public safety, or the environment, all information that could enable the public to understand or take measures to prevent or mitigate harm

arising from that threat, whether the threat is due to natural causes or human activities, including by actions of the state or by actions of private companies.

(2) Other information, updated regularly, on natural resource exploitation, pollution and emission inventories, environmental impacts of proposed or existing large public works or resource extractions, and risk assessment and management plans for especially hazardous facilities."

Principle 37 deals with protected disclosures.

Disclosure by public personnel of information, regardless of its classification, which shows wrongdoing that falls into one of the following categories should be considered to be a "protected disclosure" if it complies with the conditions set forth in Principles 38–40. Such a protected disclosure may pertain to wrongdoing that has occurred, is occurring, or is likely to occur.

"*(a) criminal offenses;*

(b) human rights violations;

(c) international humanitarian law violations;

(d) corruption;

(e) dangers to public health and safety;

(f) dangers to the environment;

(g) abuse of public office;

(h) miscarriages of justice;

(i) mismanagement or waste of resources;

(j) retaliation for disclosure of any of the above listed categories of wrongdoing; and

(k) deliberate concealment of any matter falling into one of the above categories."

Such disclosures are to be protected from retaliation, as defined in Principle 41. Public personnel who make disclosures of information showing wrongdoing, regardless of whether the information is classified or otherwise confidential, so long as, at the time of the disclosure: (i) the person making the disclosure had reasonable grounds to believe that the information disclosed tends to show wrongdoing that falls within one of the categories set out in

Principle 37; and (ii) the disclosure complies with the conditions set forth in Principles 38-40.

A core feature of this model is the ability to make disclosure to an oversight body. This is in Principle 39: Procedures for Making and Responding to Protected Disclosures Internally or to Oversight Bodies.[46]

See further below on the model's public interest defence.

G. Necessity and other defences

It is clear from the tortured discussion in the learned paper and in *Shayler* [2002] UKHL 11, that Necessity is not fit for purpose here and is not a workable option. The Public Interest defence—is not adequately dealt with in the Law Commission paper. We need to consider carefully protection for sources and journalists and this has not been done—although professional secrecy for legal advice is accepted. Proper thinking need to be applied and the views of senior media lawyers sought on the scope of appropriate defences.

---

[46] *"**A. Internal Disclosures** The law should require public authorities to establish internal procedures and designate persons to receive protected disclosures. **B. Disclosures to Independent Oversight Bodies** (1) States should also establish or identify independent bodies to receive and investigate protected disclosures. Such bodies should be institutionally and operationally independent from the security sector and other authorities from which disclosures may be made, including the executive branch.*
(2) Public personnel should be authorized to make protected disclosures to independent oversight bodies or to another body competent to investigate the matter without first having to make the disclosure internally.
(3) The 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 the power to require that testimony is given under oath or affirmation.
***C. Obligations of Internal Bodies and Independent Oversight Bodies Receiving Disclosures** If a person makes a protected disclosure, as defined in Principle 37, internally or to an independent oversight body, the body receiving the disclosure should be obliged to:(a) investigate the alleged wrongdoing and take prompt measures with a view to resolving the matters in a legally-specified period of time, or, after having consulted the person who made the disclosure, to refer it to a body that is authorized and competent to investigate; (2) protect the identity of public personnel who seek to make confidential submissions; anonymous submissions should be considered on their merits; (3) protect the information disclosed and the fact that a disclosure has been made except to the extent that further disclosure of the information is necessary to remedy the wrongdoing; and (4) notify the person making the disclosure of the progress and completion of an investigation and, as far as possible, the steps taken or recommendations made."*

The Tshwane model proposes the defence at Schedule 1 below for public servants:

The defence for citizens and the media is as set out below.

"*Principle 47: Protection against Sanctions for the Possession and Dissemination of Classified Information by Persons Who Are Not Public Personnel*
(a) A person who is not a public servant may not be sanctioned for the receipt, possession, or disclosure to the public of classified information.
(b) A person who is not a public servant may not be subject to charges for conspiracy or other crimes based on the fact of having sought and obtained the information.
Note: This Principle intends to prevent the criminal prosecution for the acquisition or reproduction of the information. However, this Principle is not intended to preclude the prosecution of a person for other crimes, such as burglary or blackmail, committed in the course of seeking or obtaining the information.
Note: Third party disclosures operate as an important corrective for pervasive over-classification.
Principle 48: Protection of Sources
No person who is not a public servant should be compelled to reveal a confidential source or unpublished materials in an investigation concerning unauthorized disclosure of information to the press or public.
Note: This Principle refers only to investigations concerning unauthorized disclosure of information, not to other crimes."

We urge the Commission to adopt this defence or a similar model.

H. Conclusion

We are grateful for the chance to participate in this consultation and would appreciate being kept informed as the issue progresses.

Yours faithfully,

Victoria McEvedy
McEvedys

Schedule 1

43: Public Interest Defence for Public Personnel

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

Note: This Principle applies to all disclosures of information that are not already protected, either because the information does not fall into one of the categories outlined in Principle 37 or the disclosure contains information that falls into one of the categories outlined in Principle 37 but was not made in accordance with the procedures outlined in Principles 38-40.

(b) In deciding whether the public interest in disclosure outweighs the public interest in non-disclosure, prosecutorial and judicial authorities should consider:

(i) whether the extent of the disclosure was reasonably necessary to disclose the information of public interest;

(ii) the extent and risk of harm to the public interest caused by the disclosure;

(iii) whether the person had reasonable grounds to believe that the disclosure would be in the public interest;

(iv) whether the person attempted to make a protected disclosure through internal procedures and/or to an independent oversight body, and/or to the public, in compliance with the procedures outlined in Principles 38-40; and

(v) the existence of exigent circumstances justifying the disclosure.

Note: Any law providing criminal penalties for the unauthorized disclosure of information should be consistent with Principle 46(b).This Principle is not intended to limit any freedom of expression rights already available to public personnel or any of the protections granted under

Principles 37-42 or 46.

Principle 46: Limitations on Criminal Penalties for the Disclosure of Information by Public Personnel

(a) The public disclosure by public personnel of information, even if not protected by Part VI, should not be subject to criminal penalties, although it may be subject to administrative sanctions, such as loss of security clearance or even job termination.

(b) If the law nevertheless imposes criminal penalties for the unauthorized disclosure of information to the public or to persons with the intent that the information will be made public the following conditions should apply:

(i) Criminal penalties should apply only to the disclosure of narrow categories of information that are clearly set forth in law;

Note: If national law provides for categories of information the disclosure of which could be subject to criminal penalties they should be similar to the following in terms of specificity and impact on national security: technological data about nuclear weapons; intelligence sources, codes and methods; diplomatic codes; identities of covert agents; and intellectual property in which the government has an ownership interest and knowledge of which could harm national security.

(ii) The disclosure should pose a real and identifiable risk of causing significant harm;

(iii) Any criminal penalty, as set forth in law and as applied, should be proportional to the harm caused; and

(iv) The person should be able to raise the public interest defence, as outlined in Principle 43."