IN THE MATTER OF AN APPEAL TO THE FIRST TIER TRIBUNAL (INFORMATION RIGHTS) UNDER SECTION 57 OF THE FREEDOM OF INFORMATION ACT 2000

Appeal No. EA/2018/0170

BETWEEN: -

PRIVACY INTERNATIONAL

Appellant

and

(1) THE INFORMATION COMMISSIONER

First Respondent

and

(2) POLICE AND CRIME COMMISSIONER FOR WARWICKSHIRE

Second Respondent

OPEN SKELETON ARGUMENT OF THE POLICE AND CRIME COMMISSIONER FOR WARWICKSHIRE

A. PRELIMINARY MATTERS/INTRODUCTION

1. This skeleton argument adopts the bundle reference system set out in Section A of the Appellant's skeleton argument. The Appellant's time estimate of 2 days for the hearing is agreed and efforts will be made to agree a timetable. The pre-reading proposed by the Appellant in Section A of its skeleton argument is agreed, save that the Tribunal is also requested to read the Closed evidence/submissions filed by the MPS and the PCC.

2. The Second Respondent, the Police and Crime Commissioner for Warwickshire **('PCC'),** is the lead respondent for those appeals where the Information Commissioner **('IC')** considered substantive, rather than 'Neither Confirm nor Deny' exemptions. The Commissioner of Police of the Metropolis **('MPS'**) is the lead respondent for the NCND appeals.

3. The appeal arises from the Appellant's FOIA request to the PCC 1st November 2016 **[1B/95-96]** for information on Covert Communications Data Capture **('CCDC')** equipment**.** The Appellant's FOIA request comprised four requests, but only requests 1-3 are in issue in this appeal. The PCC identified that the only document responsive to those requests is a Business Case for the replacement of CCDC equipment **[1B/97]**.

4. The request referenced the content of the Confidential section of the Warwickshire and West Mercia Police Alliance Governance Group meeting on 26th May 2016 **[2/150-152]**. As set out in the Open witness statement of Detective Superintendent Andrew Nolan **('AN')** of Warwickshire Police **[1B/158]**, the Confidential section of the minutes was inadvertently published without redactions by the West Mercia PCC on its website. When the error was realised, the minutes were immediately taken down and properly redacted, but not before they were re-posted by the media. As a consequence of this error, the PCC relied on substantive FOIA exemptions rather than the NCND exemptions.

5. In her Decision Notice **('DN')** of 10th July 2018 **[1B/1-12]**, the IC upheld the PCC's reliance on s. 24 (1) FOIA. Although she did not formally adopt the PCC's position in respect of the s. 31 (1) (a) and (b) exemptions, she "*would anticipate that she would support additional reliance…on s. 31 (*1)" **[1B/54].**

6. The Appellant's skeleton argument contains only about four paragraphs specific to this appeal (as opposed to the NCND appeals, in respect of which various errors of law by the IC are alleged). The Appellant summarises its position in respect of this appeal at par. 6 of its skeleton argument. In summary, the PCC responds as follows:

    (a) The Appellant's generalised contention (that s. 24 (1) and s. 31 (1) exemptions are not engaged at all) is unarguable;

(b) The IC adopted the correct approach in balancing the public interest and rightly concluded that the public in disclosure "clearly" does not match the public interest in withholding the Business Case;

(c) The same outcome is properly reached when applying the s. 31 (1) exemption.

7. The PCC endorses/supports the submissions filed by the MPS in respect of the other joined lead appeal. Insofar as is relevant to this appeal, the PCC relies on the witness evidence filed by the MPS in the other appeal.

8. Insofar as possible, the PCC will deal with the appeal in Open submissions, but it will be necessary to hear a portion of evidence and submissions in Closed session to fairly dispose of the appeal. A Closed skeleton argument is therefore also filed. The Tribunal is requested to make its decision with reference to the totality of the evidence, both Open and Closed. The Tribunal is requested to allocate time for a Closed hearing pursuant to r.35 of the Tribunal Procedure (First-tier Tribunal) (General Regulatory Chamber) Rules 2009 ("the FTT Rules") to consider the closed evidence and hear submissions. The PCC will seek to agree a timetable providing for the Closed hearing with the other parties.

9. The Appellant indicates in its skeleton argument (par. 14) that it is unlikely to seek to cross-examine AN. However, to ensure the fairness of the proceedings, AN will attend to enable the Tribunal to probe his evidence during the Closed hearing.

B. LEGAL FRAMEWORK

10. In respect of the s. 24 (1) FOIA exemption, the PCC adopts the IC's summary of the legal framework and principles as set out in par. 21-29 of the DN **[1B/7-8]** and in paragraphs 18-19, 23 of her Response **[1B/49-50].**

11. In *Quayum v. IC & Foreign and Commonwealth Office* [2012] 1 Info LR 332 at par 43-44, the Tribunal commented on the weight to be afforded to a respondent's considered view in s. 24 cases and on the relevance of considering the extent of the perceived threat:

> 43. … national security is predominantly the responsibility of the government and its various departments. The Second Respondent has contended, correctly in the Tribunal's view, that the Tribunal must at least initially afford due weight to what is regarded as the considered view of such departments, even though the exemption entails an element of public interest and the balancing test. In particular, and again the Tribunal endorses this approach, particular weight should be afforded to the views of the government or its appropriate department with regard to its or their assessment of what is required to safeguard national security in any given case and the prejudice likely to result from disclosure"; and
>
> 44. ... the Tribunal is equally firmly of the view in accepting the contention advanced by the Second Respondent that the particular weight to be applied in favour of maintaining the exemption will be proportionate to the severity of the perceived threat. Thus, to take the point which is in issue here it can with some justification, in the Tribunal's judgment, be argued that since the proliferation of WMD would constitute one of the severest threats to the security of the state, given its potential wide-ranging effect, so must the countervailing public interest in disclosure be a weighty one, such that disclosure becomes a viable option. The Tribunal stresses that nothing that has just been said in any way converts the present exemption into an absolute one".

12. The considerable weight attaching to public interest arguments in favour of maintaining the s.24 exemption is also set out in the Ministry of Justice's 2012 Guidance on s.24:

> There is obviously a very strong public interest in safeguarding national security. If non-disclosure is required to safeguard national security it is likely to be only in exceptional circumstances that consideration of other public interest factors will result in disclosure. The balance of the public interest in disclosure will depend in part on the nature and likelihood of the potential risk to national security, as well as the nature of the countervailing public interest considerations in making the information available. Each request for information will need to be judged on a case-by-case basis.

13. The PCC further draws the Tribunal's attention to the case of *Mathieson v IC and the Chief Constable of Devon and Cornwall* (EA/2010/0174), which considered s. 24 and s. 31 exemptions in the context of a request for locations of fixed automatic number plate recognition (ANPR) cameras and CCTVs operated by Devon and Cornwall Police. Due to the nature of concerns expressed by the appellant in that case (the 'capture' of innocent persons' data on a large scale) and the concerns about disclosure expressed by the police (risk of compromising the effectiveness of a crime-fighting technology), the Tribunal's analysis at par. 10 of *Mathieson* is of particular relevance:

> All these points have some validity and we accept that disclosure of the requested information may only have tipped the scales in favour of terrorists and serious organised criminals slightly. But we are bound also to take account of the fact that, although the risk may have been small, if disclosure of the information requested meant, for example, that a terrorist incident took place which might otherwise have been avoided, the results could be catastrophic. We have considerable sympathy with Mr Middleton's plea that the police ' ... need to stay one step ahead' and with his rhetorical question: 'Why would we want to give one of our tools back to the criminals?"

14. As the IC did not formally reach a decision in respect of the s. 31 (1) (a) and (b) exemptions, the PCC highlights the guidance in *Hogan and Oxford City Council v IC* (EA/2005/0026) in respect of analysing s. 31 'prejudice':

> 29 First, there is a need to identify the applicable interest(s) within the relevant exemption. There are only two under s31(1)(a), namely the prevention or detection of crime.
>
> 30 Second, the nature of the 'prejudice' being claimed must be considered. An evidential burden rests with the decision maker to be able to show that some causal relationship exists between the potential disclosure and the prejudice and that the prejudice is, as Lord Falconer of Thoronton has stated, "real, actual or of substance" (Hansard HL, Vol. 162, April 20, 2000, col. 827). If the public authority is unable to discharge this burden satisfactorily, reliance on 'prejudice' should be rejected. There is therefore effectively a de minimis threshold which must be met. Oxford sought the advice of the DVLA and Thames Valley Police.

They advised that the disclosure of VINs together with the other information sought could be used to clone vehicles. We are satisfied that Oxford established such a causal relationship.

31 When considering the existence of 'prejudice', the public authority needs to consider the issue from the perspective that the disclosure is being effectively made to the general public as a whole, rather than simply the individual applicant, since any disclosure may not be made subject to any conditions governing subsequent use.

32 However, while the intended use or motive of the applicant is not relevant to a decision whether to grant or refuse access this Tribunal accepts that where a public authority is aware of the intended use, it may be a factor for consideration when assessing the nature of the prejudice. In this appeal there appears to have been a mistaken belief as to the possible intended purpose, which was unsubstantiated and wrong, and therefore the Tribunal considers it is not a factor which should have been taken into account by Oxford…

34 A third step for the decision-maker concerns the likelihood of occurrence of prejudice. A differently constituted division of this Tribunal in John Connor Press Associates Limited v Information Commissioner (EA/2005/0005) interpreted the phrase "likely to prejudice" as meaning that the chance of prejudice being suffered should be more than a hypothetical or remote possibility; there must have been a real and significant risk…

35 On the basis of these decisions there are two possible limbs on which a prejudice-based exemption might be engaged. Firstly, the occurrence of prejudice to the specified interest is more probable than not, and secondly there is a real and significant risk of prejudice, even if it cannot be said that the occurrence of prejudice is more probable than not. We consider that the difference between these two limbs may be relevant in considering the balance between competing public interests (considered later in this decision). In general terms, the greater the likelihood of prejudice, the more likely that the balance of public interest will favour maintaining whatever qualified exemption is in question.

C. **SUBMISSIONS**

Engagement of s. 24 (1) in respect of the Business Case

15. The threshold question for the application of s. 24 (1) is whether non-disclosure of the Business Case is required (interpreted as "reasonably necessary" in *Kalman v Information Commissioner and the Department of Transport (*EA/2009/0111)) for the purpose of safeguarding national security.

16. 'National security' is broadly defined as the security of the United Kingdom and its people, not limited to actions targeted at the UK or its government (*Norman Baker v. IC and the Cabinet Office* (EA/2006/0045) with reference to *Secretary of State for the Home Department v. Rehman* [2001] UKHL 47).

17. In addition to traditional threats to national security (such as espionage and terrorism), there exist threats to national security emanating from serious organised criminality. This is recognised by the 2018 Serious Organised Crime Strategy which states:

> *Serious and organised crime affects more UK citizens, more often, than any other national security threat and leads to more deaths in the UK each year than all other national security threats combined*.[1]

18. AN's evidence (par. 9-11) **[1B/159-160]** is that "*elements of organised crime directly impact national security*". The PCC submits that the definition of 'national security' is sufficiently wide that some, if not all, of the work done by the West Midlands Regional Organised Crime Unit ('**ROCU'**) falls within its ambit.

19. AN's Open WS at par. 16 gives his professional evaluation that:

> *Due to the details contained in the document, if the business case was to be disclosed, it would allow terrorists and criminal networks to build up a picture of different forces' abilities to respond to the activities of these groups and thus increase the threat to the public.*

[1] https://www.gov.uk/government/publications/serious-and-organised-crime-strategy-2018

20. The National Threat Level, since September 2017, has been designated SEVERE ('*an attack is highly likely')*.[2] As the IC observed in par. 28 of her Response **[1B/51]**, "*the nature of counter-terrorism (and indeed organised and serious crime) investigations…are likely to involve sophisticated suspects".* This serves to increase the risks arising from disclosure of information about police technology/techniques.

21. At par. 14 of its skeleton argument, the Appellant observes that "*it is difficult to go behind these [senior police officers'] assertions of risk, as the evidence upon which they are based has not been revealed*." Although the Tribunal is better placed to probe the officers' evidence/assessments during the Closed hearing, given the officers' specialist expertise and knowledge, the Tribunal should pause and reflect very carefully before overriding the sincerely held view of the senior officers (per *Quayum).* There appears to be no dispute that these concerns are, indeed, sincerely held (even if the Appellant considers them to be 'overstated').

22. At par. 25 (c) of the Appellant's skeleton argument, it contends that the s. 24 exemption does not apply because "*there is no suggestion that this confirmation [of the PCC holding a Business Case] impacted on national security in any way".* In this case, absence of evidence is not evidence of absence. It is unrealistic to expect concrete evidence of how such a disclosure (of limited information within the erroneously unredacted Minutes) impacted criminals' operations or tactics. Organised crime or terrorist groups do not complete feedback surveys or participate in studies about how their tactics change in response to information about police technologies. However, senior police officers' assessment of adverse impact provides sufficient evidence for the Tribunal to reach a view, to the necessary causation standard, of an adverse impact caused by disclosure.

23. The Respondents do not need to demonstrate a *likelihood* of prejudice to national security in order for the s. 24 (1) exemption to apply. Per *Rehman*, there need only be a "*real possibility of an adverse effect… [not an effect which is] direct or immediate*". The police evidence clearly crosses that threshold.

[2] https://www.mi5.gov.uk/threat-levels

Engagement of s. 31 (1) (a) and (b)

24. The IC, in spite of not having formally considered s. 31 as part of the DN (having upheld reliance on s. 24 (1)), indicates in par. 45-46 of her Response **[1B/54]** that she "*anticipates that she would support additional reliance by the Forces*" on s. 31 (1).

25. The Appellant's Reply **[1B/64]** and Skeleton Argument (par. 6 (b)) assert that s. 31 "*does not apply*" but no basis for this bold assertion is cited. The suggestion that criminals' knowledge of police technology and techniques would not give rise to a real/significant risk of prejudice to policing is unrealistic. Information about details of law enforcement agencies' technology fall squarely within the realm of Public Interest Immunity as demonstrated by the courts consistently finding that policing techniques attract PII. As *per* Lord Bingham in *R v H* [2004] 2 AC 134 at [18], public interest immunity would attach to information such as *"the use of […] operational techniques (such as surveillance) which cannot be disclosed without … jeopardising the success of future operations"*. This approach was applied in *R. (on the application of Metropolitan Police Service) v Chairman of the Inquiry into the Death of Azelle Rodney* [2012] EWHC 2783 (Admin) at [33-5]. FOIA should not create a bypass through the protections afforded to such material in the context of criminal investigations/proceedings.

26. Par. 30 of the Appellant's skeleton argument states that s. 31 is not engaged because "*it does not inherently follow that disclosing this business case reveals information that would negatively impact upon national security or on policing purposes."* Whether or not such an 'inherent' effect exists, the PCC does not make a bare assertion to that effect; he relies on evidence showing the likelihood of prejudice to those police functions (alternatively, a real and significant risk of such prejudice) if the Business Case was disclosed. This includes AN's evidence of increasing tech-savviness of offenders **[1B/160]**.

27. Section 31 (1) is engaged because, for the reasons set out in AN's two witness statements, disclosure of the Business Case would or would be likely to prejudice the prevention or detection of crime and apprehension or prosecution of offenders. There is, as recognised by the IC, "*very considerable overlap with the basic point made in support of reliance on section 24*" **[1B/54].**

Impact of information in public domain

28. The Appellant places significant emphasis on information (purportedly describing the use and capabilities of CCDC equipment) in the public domain. However, AN's evidence (on reviewing the information put forward by the Appellant) is that "*in my opinion …much of the information…is speculative"* **[1B/159]**.

29. The Appellant approaches this issue in a binary way: either information about CCDC is publicly available or it is not. However, the issue is far more nuanced: the extent and specificity of the information, the level of certainty and correctness are highly relevant. The PCC is unable to make detailed Open submissions in this respect, but highlights the Information Commissioner's Office Guidance *Information in the Public Domain*[3], which provides a framework for analysing 'public domain' issues including with reference to:

(i) Whether the requested information is more detailed than that already in the public domain (*Craven v Information Commissioner* (EA/2008/0002)). In this instance, AN's acknowledges that the unredacted Minutes contained some information but notes that disclosure of the Business Case "*would mean specific detail being known. There is a big difference between knowledge of the existence of a business case*" and knowledge of its contents **[1B/159]**;

(ii) Whether disclosure could corroborate a previously unreliable source or leak, give previously unknown context for the information, or establish that no further information exists on a topic (*PETA v Information Commissioner and University of Oxford* (EA/2009/0076, 13 April 2010));

(iii) The ease with which the information can be found and used: information may technically be in the public domain even if it is hidden or buried within a mass of other material or would take some time and effort to find and collate. Disclosure of that information in a more organised or easily usable form may draw more attention to it or increase the risk of misuse (*PETA)*.

3 https://ico.org.uk/media/1204/information-in-the-public-domain-foi-eir-guidance.pdf

30. It is relevant that the Confidential Section of the Alliance Meeting Minutes was disclosed in error and that error was remedied once it became known. This was not a deliberate disclosure.

31. At paragraph 19 (d) of the Appellant's skeleton argument, it is said that UK police forces have disclosed information about other covert surveillance techniques such as mobile extraction and hacking. No meaningful comparison can be drawn with these techniques. Mobile phone extraction is not a surveillance technique. Hacking is subject to Regulation of Investigatory Powers Act 2000 and its capabilities are widely known. The availability of information about one technology does not mean that disclosure in respect of another would not be damaging to national security/law enforcement.

32. To avoid unnecessary repetition, the PCC notes and adopts the MPS' analysis of the information said to be in the public domain, as set out in its Open skeleton argument.

33. In the PCC's submission, the Tribunal's assessment of prejudice/harm arising from disclosure of the Business Case is not substantially assisted by examination of information in the public domain.

Public interest balancing

34. In respect of the s. 24 (1) exemption, although it does not carry 'inherent weight', within the context of this case there must be a fair recognition of the considerable public interest involved in protecting national security. This was recognised by the Upper Tribunal in *Keane v. IC, Home Office and Metropolitan Police Service* [2016] UKUT 461 (AAC) at par. 58:

> *the reality is that the public interest in maintaining the qualified national security exemption in section 24 (1) is likely to be substantial to require a compelling competing public interest to equal or outweigh in.*

35. In respect of both s. 24 (1) and s. 31 (1) exemptions, the public interest in maintaining those exemptions must be analysed in light of how serious the potential harm from disclosing the Business Case is. In the context of a request concerning airport passenger search procedures, the Tribunal in *Kalman* recognised (at par. 47) that even if the risk of a particular harm occurring is relatively low, the seriousness of the consequences of that risk coming to pass can mean that the public interest in avoiding

the risk is very strong. It is submitted that this analysis applies equally to s. 31 (1), where, as is often the case with serious criminality, lives may be at stake.

36. Both *Quayum* and *Mathieson* emphasise the need to give due regard to the severity of the consequence if the risk came to pass, even if that risk was small (i.e. 'just tipping the scales' in favour of criminals/terrorists). The PCC contends that, in respect of disclosing the Business Case, the risk is not a small one.

37. The Appellant places significant reliance on information about how CCDC equipment is used internationally. It is asserted that greater disclosure in certain jurisdictions did not lead to harm to policing, but no evidence is put forward to prove this negative. Without any criticism of the Appellant, it must be observed that its witnesses' opinion evidence does not come from an impartial source and is insufficiently rigorous to draw any meaningful conclusions. Furthermore, just because other countries chose a particular approach to disclosure of information on CCDC use, does not mean that it is the correct approach (either generally or for England/Wales specifically). The Tribunal will also note that Mr. Wessler and Mr. Buermeyer are not law enforcement professionals and do not have experience of policing in this country, unlike the Respondents' witnesses.

38. Even if these assertions were accepted at face value, the Appellant's information focuses on Germany and the United States; it does not purport to be a study of all jurisdictions where such technology is used, the level of information available and any resulting impact on policing. Jurisdictions differ in respect of policing, criminality and oversight of surveillance. It would not, in the PCC's submission, be safe to draw any meaningful inference from the limited examination of a small comparator pool.

39. The Appellant at par. 16 of its skeleton argument invites the Tribunal to discount the police officers' open evidence about the oversight regime because the level of safeguards "*would need to be proportionate to the level of intrusion*". However, in the event of CCDC use, those involved in its oversight *would* have the full information about the level of intrusion and the reasons why it is required in each case. Consideration of the Human Rights Act 1998 is integral to this process, of which proportionality is part and parcel. In most cases, prior authorisation from the Judicial Commissioner would be obtained, save in cases of urgency (where the Commissioner must review the matter within 5 days) **[1B/195].**

40. DS Williams' and AN's open WS set out the internal and external control mechanisms which would apply in the event of such equipment being used. In *Kennedy v Charity Commission* [2015] AC 455, the Supreme Court had accepted that, even in the absence of prior judicial authorisation, the existence of independent oversight (including by the Commissioner) did provide adequate safeguards against abuse (par. 167-169). In a recent judgment, the Divisional Court in *R (National Council for Civil Liberties) v Secretary of State for the Home Department* [2019] EWHC 2057 (Admin) rejected a Human Rights Act 1998 challenge to the safeguards offered by the Investigatory Powers Act 2016. Further, there exists the additional safeguard that decisions of the IPT are amenable to judicial review (*R (Privacy International) v Investigatory Powers Tribunal* [2019] 2 W.L.R. 1219).

41. The existence of this robust and independently supervised system (which includes consideration of proportionality in each case) significantly undermines the Appellant's argument that the need for greater public/media scrutiny is so overwhelming that policing concerns are outweighed. The existence of a sufficient oversight system is more important to the assessment of public interest in disclosure of the Business Case than the identity of that 'overseer' (whether the media/public or independent specialist bodies).

42. The Appellant at par. 28 (iii) of the skeleton argument contends that the existing public debate about the use of such equipment does not take away from the public interest in disclosure because it has not been a properly informed debate "*based on actual awareness of the extent of their use*". Once again, the Appellant incorrectly adopts a binary approach: either there is absolute disclosure of all information on use/capabilities of the equipment, or the public debate is so lacking that its existence should not weigh in the balance at all. In a perfect world, all public debates would take place in full possession of all the underlying facts; in the real world, that rarely is the case. The existence of a public debate on this issue, whether or not it is fully informed by all the facts, was a valid factor for the IC to weight in the balance.

43. The Appellant at paragraphs 8 and 25 (c) of its skeleton argument contends that its status as a 'public watchdog' creates an entitlement pursuant to Article 10 ECHR to access the withheld material and is a factor of 'particular weight' in a public interest balancing exercise. This submission is incorrect, for the following reasons:

(i) In *Kennedy*, the Supreme Court decided that Article 10 does not give rise to a freestanding right of access to information held by public authorities. Although Lord Mance (giving the lead judgment) acknowledged (at para. 42 and 57) that his conclusion on this issue was not essential to the Court's decision, the point was fully argued and considered in great depth in his judgment, at paras. 57-100, as well as in Lord Toulson's judgment at paras. 143-150. In the circumstances, the Tribunal should not depart from the Supreme Court's thorough analysis and conclusions. It would not be appropriate for this Tribunal to address the question as to the extent to which the Supreme Court's conclusions in *Kennedy* ought to be revisited in light of the subsequent developments in the Strasbourg caselaw (including the case of *Magyar* on which the Appellant relies). *Kennedy* provides a clear and complete answer to the Appellant's reliance on Article 10. The First Section of the European Court of Human Rights has, in 2018, rejected Mr. Kennedy's appeal (on a procedural ground);

(ii) In *Magyar,* no general Article 10 entitlement to receive information held by a government was found. When considering situations where an entitlement could arise, the Grand Chambers outlined a number of indicative factors (at par. 157), 'public watchdog' status being only one of them;

(iii) Even if Article 10 was engaged by the request, it would make no difference to the outcome of this case. This is because Article 10 rights are subject to the restrictions in Article 10 (2) including those in the interests of national security, public safety and for the prevention of disorder or crime. Article 10 would also need to be balanced against the rights of others, including Article 2 and 3 rights of individuals adversely affected by the disclosure. As the exemptions relied on by the PCC are not absolute (as was the case in *Kennedy*) but involved a balancing exercise, Article 10 and the Appellant's status makes no material difference to outcome. This is in line with the decision in *Quayum,* where the Tribunal determined that Article 10 would make no difference to the analysis, given the checks and balances built into the meaning of s. 24 and the public interest test;

(iv) The FOIA is generally applicant-blind (save where a request is said to be vexatious, in which case 'motive' may be relevant) and any disclosure is 'to the world', so the Appellant's status is not a material factor. The IC at par. 41 of the DN **[1B/10]** was correct in discounting the nature of the Appellant's organisation from her analysis. The legitimacy of the Appellant's (and the public's) interest in

the information was accepted by the PCC and the IC—but that public interest was outweighed by competing public interests.

44. The question asked in *Mathieson*, 'why would we want to give one of our tools to the criminals?' is particularly resounding in the present case. The risk of severe consequences from the Business Case becoming public clearly requires the public interest balance to favour the exemptions.

D. CONCLUSIONS

45. The Tribunal is invited to uphold the DN and dismiss this appeal for the reasons given.

Alex Ustych
5 Essex Court
6 August 2019