

Neutral Citation Number: [2026] UKIPTrib 9

Case Nos: IPT/26/191/CH and IPT/25/83-86/CH

IN THE INVESTIGATORY POWERS TRIBUNAL

Royal Courts of Justice
Strand, London, WC2A 2LL

Date: 19 November 2026

Before :

LADY CARMICHAEL (PRESIDENT)
MR JUSTICE CHAMBERLAIN
and
MR JUSTICE JOHNSON

- -

Between :

IPT/26/191/CH	**Apple Inc.**	**Claimant**
	- and -	
	Secretary of State for the Home Department	**Respondent**
	And Between :	
IPT/25/83-86/CH	**(1) Privacy International** **(2) Liberty** **(3) Ian Hosein** **(4) Ben Wizner**	**Claimants**
	- and -	
	Secretary of State for the Home Department	**Respondent**

- -
- -

Daniel Beard KC, Julian Milford KC, Gayatri Sarathy and **Raphael Hogarth** (instructed by Fieldfisher) for the Claimant in case IPT/26/191/CH

Ben Jaffey KC, Celia Rooney and **Abe Chauhan** (instructed by Leigh Day) for the Claimants in case IPT/25/83-86/CH
Neil Sheldon KC, Christopher Knight KC, Karl Laird and Hugo Murphy (instructed by Government Legal Department) for the Respondent
Jason Beer KC and **Paul Skinner** (instructed by the Tribunal) as Counsel to the Tribunal

Hearing date: 17 September 2026

JUDGMENT

Lady Carmichael, Mr Justice Chamberlain and Mr Justice Johnson:

1. This judgment concerns two separate claims and complaints. We adopt the shorthand used by counsel, and refer to the claimants in the two claims as "Apple" and "the NGOs". We refer to the claims and complaints, compendiously, as "the claims".

2. The claims raise issues as to the Secretary of State's powers to give a "relevant operator" a "technical capability notice" under section 253 of the Investigatory Powers Act 2016. The respondent says that it would be damaging to national security if she is required publicly to confirm or deny whether a technical capability notice has been given to Apple. The claimants disagree and say that the open justice principle requires that this central feature of the case is not kept secret. They say it is already clear from what is in the public domain that a technical capability notice has been given to Apple, and that it could not conceivably damage national security for that fact to be confirmed in these proceedings. In the event that Apple has been given a technical capability notice, there is then a further issue as to whether its content should be publicly revealed in these proceedings.

3. We heard submissions from Daniel Beard KC for Apple, Ben Jaffey KC for the NGOs, Neil Sheldon KC for the respondent and Jason Beer KC as counsel to the Tribunal.

4. The hearing was divided into three components. The OPEN component was heard in public, with all parties represented. There was then a PRIVATE component, with the NGOs excluded and with Mr Beer advancing submissions

that supported their interests. A CLOSED hearing also took place, with the NGOs and Apple excluded and with Mr Beer advancing submissions supporting their interests.

5. We are handing down separate PRIVATE and CLOSED judgments at the same time as this judgment. The substance of our decision and reasoning is set out in this judgment. The PRIVATE and CLOSED judgments contain additional details that cannot be published without damaging the public interest. The Tribunal is therefore prevented from publishing those judgments by rule 7 of the Investigatory Powers Tribunal Rules 2018.

The facts

Apple's first claim

6. In early 2025 Apple brought a claim against the respondent. At the time, the respondent said the existence of the claim must be kept secret and any hearing should not be published in the daily case list. The Tribunal disagreed. It listed a hearing and the court listing was published on the Tribunal's website. The listing did not reveal the parties' identities, so as not to pre-judge the respondent's arguments that they should be kept secret. After a hearing, which also had OPEN, PRIVATE and CLOSED components, the Tribunal rejected the respondent's contention that the identity of the parties should be kept secret. It also rejected the respondent's contention that the subject matter of the claim should be kept secret. It was therefore publicly revealed that the claim had been brought by Apple against the Secretary of State for the Home Department and that it concerned the power to give a relevant operator a technical capability

notice. The Tribunal's reasons are set out in OPEN, PRIVATE and CLOSED judgments dated 7 April 2025. Shortly thereafter, the NGOs commenced their claim. The NGO claim was listed for a substantive hearing in December 2026.

7. Apple's claim was subsequently dismissed because of a change of circumstances. In July 2026 Apple commenced this second claim.

8. A case management hearing was listed, in part to determine whether a trial could still take place in December 2026 and what further directions were necessary. The parties agree that a substantive hearing in December 2026 is impractical. They indicate they are likely to be able to agree case management directions with a view to a substantive hearing in the first half of 2027. The principal issue between the parties which the Tribunal is asked to resolve is whether it would damage the public interest to reveal if the respondent has given a technical capability notice to Apple, and, if so its content. The resolution of that issue is likely to impact on the extent to which the substantive hearing can take place in OPEN. It will also affect the extent to which evidence can be exchanged in OPEN as opposed to PRIVATE or CLOSED.

Media reporting, public comment and correspondence with the Tribunal

9. There has been extensive media reporting to the effect that the respondent has given Apple a technical capability notice requiring it to be able to maintain access to its users' data in decrypted form, so that such data is available to be passed to intelligence agencies. That reporting, and other public comment, is summarised in the Tribunal's OPEN April 2025 judgment at paragraphs 14-19. The reporting includes a report in The Times that the Home Office issued an

order under the 2016 Act to require Apple to provide access to encrypted material, and that this had been "confirmed by Home Office sources". The public statements include statements made by Tulsi Gabbard, who was then US Director of National Intelligence, and statements attributed to the President of the USA.

10. There have been further public statements and media reporting since the April 2025 hearing.

11. On 20 July 2025, The Financial Times published an article which said that the newspaper had been told by "two senior British officials" that the Government was "seeking a way out of a clash with the Trump administration over the UK's demand that Apple provide it with access to secure customer data". It quoted an official in "the UK's technology department" as saying "This is something that the vice-president is very annoyed about and which needs to be resolved… The Home Office is basically going to have to back down."

12. On 19 August 2025, Ms Gabbard published a post on X that was viewed more than three million times:

> "Over the past few months, I've been working closely with our partners in the UK, alongside @POTUS and @VP, to ensure Americans' private data remains private and our Constitutional rights and civil liberties are protected.
>
> As a result, the UK has agreed to drop its mandate for Apple to provide a "back door" that would have enabled access to the protected encrypted data of American citizens and encroached on our civil liberties."

13. On the same day, The Financial Times published an article under the headline "UK has 'agreed to drop' demand for access to Apple user data, says US" and

the sub-headline "Move protects Americans' civil liberties, Trump's director of national intelligence Tulsi Gabbard tells FT."

14. On 1 October 2025, The Financial Times published an article under the headline "UK makes new attempt to access Apple cloud data" and the sub-headline "Order issued in September comes after Trump administration said London had backed down in fight over encryption". The article quoted the Home Office as stating that it did not comment on operational matters and would not confirm or deny the existence of any technical capability notice. However, the article also stated: "two senior British government figures said the US administration was no longer leaning on the UK government to rescind the order."

15. Shortly before the hearing, the Tribunal received a letter from US Senator Ron Wyden and US Congressman Warren Davidson. The letter was also published by The Guardian newspaper. The letter asked the Tribunal to permit greater transparency into the "the challenge reportedly filed by Apple concerning a surveillance directive from the UK government under the Investigatory Powers Act." The letter said that Apple had been authorised by the UK Government to brief certain members of the US executive and legislature about the issue:

> "Apple recently informed Congress that it is challenging the UK government's authority to issue surveillance directives. Apple sought permission from the UK government to discuss this issue in more detail with both the executive and legislative branches of the US government. Apple further informed Congress that the UK government granted Apple permission to brief the Attorney General, the Vice President, and their staff, while explicitly prohibiting the company from discussing the issue in further detail with the US Congress."

The respondent's evidence

16. The respondent relies on a witness statement of Lucy Montgomery-Pott that was served for the hearing in April 2025. Ms Montgomery-Pott is the Head of the Investigatory Powers Unit which is part of the Homeland Security Group within the Home Office. The statement was only served in PRIVATE. Ms Montgomery-Pott explains the damage to national security that she says would arise if "the fact, substance or parties to these proceedings be made public." Ms Montgomery-Pott said that there had been an investigation into the reference in The Times article to Home Office sources confirming that Apple had been ordered to provide access to encrypted material. She said that "no Government source has been identified", but provided no detail of the investigation undertaken and no copy of any investigation report. She did not identify who had been investigated, or what investigative steps had been taken (for example whether electronic devices had been examined). She did not say whether Ministers or senior officials (including special advisers) had been asked if authority had been given to brief The Times or, if they had been asked, what they said.

17. The respondent also relies on an OPEN and a PRIVATE witness statement of Andrew Scurry, the Director of Technology, Data and Innovation in the Homeland Security Group of 11 September 2026. Mr Scurry says that he agrees with and adopts the views set out by Ms Montgomery-Pott in her statement. He says that, although there has been significant media reporting and public commentary concerning "matters alleged to relate to Apple and a TCN", there is an important distinction between such reporting and confirmation by the

Government. He says that, if the Government confirmed the existence of a technical capability notice and/or its technical details, that would damage national security. It is therefore necessary for the Government to maintain its approach of neither confirming nor denying whether a technical capability notice has been issued. He says that "the NCND principle is only effective when it is maintained consistently." He claims that "Ministers and Home Office officials have consistently neither confirmed nor denied the existence, contents, scope or operational effect of any individual TCN." If that sentence were true, then the statements in The Times and The Financial Times to the contrary effect would be false.

18. Mr Scurry adopts the account of Ms Montgomery-Pott that, following publication of the article in The Times, an investigation was conducted, but without giving any further detail. In respect of the subsequent articles in The Financial Times, he says: "Both of these Financial Times articles were subject to a leak investigation by Government Security Group." Again, no further detail is given of what this investigation involved, nor indeed of what (if anything) it revealed.

19. The respondent's evidence does not include any assessment that damage had been caused to national security as a result of the Tribunal's publication, in April 2025, of a public case list that revealed the existence of a claim, or its order that revealed that the claim was brought by Apple and that it concerned the respondent's powers to give a relevant operator a technical capability notice.

Legal framework

20. The applicable legal framework is set out in the Tribunal's April judgments. We repeat part of that account here.

Open justice

21. Open justice is a fundamental common law constitutional principle which applies to all courts and tribunals exercising the state's judicial power: *Dring v Cape Intermediate Holdings Limited* [2020] AC 629 *per* Lady Hale at [41]. It applies to the Investigatory Powers Tribunal: *Various claimants v Security Service* [2022] UKIP Trib 3, [2023] 2 All ER 849 *per* Singh LJ (President) at [71]. However, the Tribunal operates in a different procedural and legislative context compared to other courts and tribunals. That difference impacts on the application of the open justice principle: *Various claimants* at [75]-[76].

The Tribunal's rules

22. Rule 7(1) of the Investigatory Powers Tribunal Rules 2018 states:

> "The Tribunal must carry out their functions in such a way as to secure that information is not disclosed to an extent, or in a manner, that is contrary to the public interest or prejudicial to national security, the prevention or detection of serious crime, the economic well-being of the United Kingdom or the continued discharge of the functions of any of the intelligence services."

Approach to claimed risks to national security

23. The executive is entitled to take a precautionary approach when assessing risks to national security. Courts and tribunals must accord particular weight to such assessments made by the executive. Those assessments should usually be

accepted, unless they are shown to be irrational or otherwise vitiated by a public law error: *Secretary of State for the Home Department v Rehman* [2001] UKHL 47, [2003] 1 AC 153 *per* Lord Hoffmann at [50] and [62], Lord Slynn at [17] and [27] and Lord Steyn at [42]; *R (Lord Carlile of Berriew QC) v Secretary of State for the Home Department* [2014] UKSC 60, [2014] AC 945 *per* Lord Sumption at [22]-[33]; *R (Begum) v Special Immigration Appeals Commission* [2021] UKSC 7 [2021] AC 765 *per* Lord Reed at [53]-[62], [70] and [109]; *Various claimants v Security Service* [2022] UKIP Trib 3, [2023] 2 All ER 849 *per* Singh LJ (President) at [47].

24. In *Attorney General v BBC; R (Beth) v Investigatory Powers Tribunal* [2025] EWHC 1669 (KB), the Divisional Court (Lady Carr CJ, Dame Victoria Sharp PKBD and Chamberlain J) said, at [19]:

> "The justification for the respect owed to [national security assessments by the executive branch of government] is in significant part based on institutional matters including the expertise and experience of the personnel involved and the wide range of sources of information available to them. However, this respect is warranted only if, and to the extent that, the courts can have confidence without reservation in the processes by which such assessments are prepared and presented."

Neither confirm nor deny policy

25. To protect the secrecy of sensitive intelligence, the Government adopts a policy of neither confirm nor deny: NCND. It is in furtherance of this policy that the Government has publicly neither confirmed nor denied whether Apple has been given a technical capability notice.

26. NCND is an important Government policy for the protection of national security: *In re Scappaticci's application for judicial review* [2003] NIQB 56 *per* Lord Carswell CJ at [15]. Its efficacy depends on it being maintained generally: Restriction order ruling in the Dawn Sturgess Inquiry *per* Lord Hughes at [15]. But it is not an absolute or blanket rule of law: "It is not simply a matter of a governmental party to litigation hoisting the NCND flag and the court automatically saluting it": *Mohamed v Secretary of State for the Home Department* [2014] EWCA Civ 559, [2014] 1 WLR 4240 *per* Maurice Kay LJ at [20].

27. The Tribunal's decision making is governed by rule 7 of the 2018 Rules. If a departure from NCND in a particular case would involve damage to national security then rule 7 requires that the Tribunal carries out its functions in a manner that would enable the Government to maintain NCND in that case. If, conversely, a departure from NCND would not involve damage to national security then rule 7 does not prevent the Tribunal from conducting an OPEN hearing which would have the effect of disclosing information to the public that the Government regards as being subject to the NCND policy.

28. In its PRIVATE April 2025 judgment (which can, in part, now be put into OPEN), the Tribunal explained why it was appropriate to publish the fact and subject matter of these proceedings and the names of the parties, notwithstanding the Government's wish to maintain NCND:

> "
>
> 53. Further, the respondent continues to retain a degree of choice and control over the maintenance of NCND. In legal

proceedings, it occasionally happens that the continuation of the proceedings requires a departure from NCND (for example the revelation of the identity of a human source in order to protect the fair trial rights of a defendant in criminal proceedings where a public interest immunity application is refused). In such cases, the authorities can decide whether to depart from NCND or whether, instead, to withdraw or compromise the underlying proceedings. [...]

54. Further, although NCND can only be effective if it is generally maintained, it is not a blanket rule and its utility is not defeated by occasional and exceptional departures from its application. There are a number of examples of departures from the NCND policy. The so-called Wilson doctrine (under which the Government indicated that it did not intercept the communications of Parliamentarians and that if that position changed Parliament would be informed at a suitable point) involves a departure from NCND in both of its aspects. In the inquest into the death of Diana, Princess of Wales, the Secret Intelligence Service denied that the Princess of Wales had been a subject of intelligence interest. The Foreign Secretary in 2012, in response to a question as to whether Nigel Heywood was a source for the Secret Intelligence Service, responded that he had not been employed by the British Government in any capacity. In 2012 the Secret Intelligence Service gave evidence as to the nature of Gareth Williams' employment by the intelligence agencies at the time of his death: Undercover Policing Inquiry, ruling on legal principles and approach, 3 May 2016 *per* Sir Christopher Pitchford at [128].

55. [...]

56. [...]

57. It follows that... the application must be dismissed...

58. Although not necessary (or, arguably, relevant) to our decision, there are further reasons why it is desirable for the bare details of the case to be public. It is likely to raise legal issues of some considerable importance, [...] It is undesirable, and injurious to the public development of legal principle, for such issues to be resolved entirely in secret. Sometimes, that has to happen, where the public revelation of a legal issue in a particular context would tend to reveal underlying facts and where the revelation of those underlying facts would be damaging to national security. For the reasons we have given, that is not the case here."

29. There is a further factor that is relevant to the issue that now arises. The utility of NCND in an individual case depends on its being maintained consistently in that case. If the Government itself has not been consistent in maintaining NCND in respect of a particular matter, the court is unlikely to give weight to an assertion that a departure from NCND would be damaging to national security. It follows that there is an obligation on a party seeking to apply NCND to ensure that the court is aware of any arguable departure from NCND. In *BBC* and *Beth* the Divisional Court said, at paragraphs 27-28:

> "27. ...it is important that a party seeking to adopt a NCND stance in relation to a fact relevant to legal proceedings ensures that the court is candidly informed (if necessary in CLOSED pursuant to a public interest immunity application or a closed material procedure) about:
>
> (a) the existence and terms of any relevant policy relating to the use of NCND and/or to the circumstances in which it may be departed from; and
>
> (b) the circumstances of any departure from NCND in the particular case or other related cases and the precise terms of the departure (including whether the departure was authorised, whether the information was conveyed in confidence and the precise terms of any departure).
>
> 28. If it is unclear whether there has been such a departure, any material which evidences or suggests that there has been must always be candidly disclosed to the court (if necessary in CLOSED pursuant to a public interest immunity application or closed material procedure). This is an incident of the duty owed by any party engaged in court proceedings to ensure that the court is able to carry out its functions on a properly informed basis...."

Submissions

30. Ben Jaffey KC, for the NGOs, submits that the Secretary of State's continued reliance on NCND as to the existence of a technical capability notice, and its

terms, is no longer tenable in the light of the extensive public reporting and official statements. He says that the sequence of events, which include the dismissal of Apple's first claim, and then the bringing of a subsequent claim, mirrors the public reporting that Apple had been issued with a technical capability notice, that this had been withdrawn following pressure from the US government, and that a new notice had then been issued. He says that it follows as a matter of irresistible inference that it is now in the public domain that the Secretary of State has given Apple a technical capability notice. It could not conceivably damage national security for that fact to be acknowledged in these proceedings. He says that the Tribunal should determine the "NCND issue" now, because the respondent's reliance on NCND materially impairs open justice and the claimants' ability to make submissions, obtain disclosure and rely on expert evidence.

31. Daniel Beard KC, for Apple, was constrained in what he could say in OPEN pending the Tribunal's resolution of this issue. He submitted that Apple should have permission to refer openly to "certain key facts" in these proceedings, including whether the respondent has, in fact, given Apple a technical capability notice. He says that open justice, fairness and the extensive public reporting that has now taken place justify greater transparency and would not damage national security. He says that Apple would otherwise be unfairly prevented from publicly advancing facts it knows to be true.

32. Neil Sheldon KC, for the respondent, submits that NCND should continue to be maintained because its effectiveness as a policy to protect national security depends on its consistent application. Official confirmation or denial of the

existence of a technical capability notice in this case would create a damaging precedent for future national security cases. He argues that there is a critical distinction between media speculation and formal confirmation or denial by Government. The Tribunal should give substantial weight to the Home Office assessment that public disclosure of the true position would damage national security, and that the balance falls decisively in favour of protecting national security.

33. Jason Beer KC, as counsel to the Tribunal, did not advance substantive submissions in OPEN. In the PRIVATE part of the hearing, he supported the submissions that were advanced in OPEN by the NGOs and contended that the PRIVATE (and CLOSED) evidence advanced by the respondent did not establish that it would be damaging to national security to reveal whether a technical capability notice had been given to Apple. He pointed out that the respondent's documents which explain the true position are marked "OFFICIAL SENSITIVE" rather than "SECRET" or "TOP SECRET", which he said was inconsistent with the respondent's contention that their disclosure would be damaging to national security.

Would it be damaging to national security to reveal whether the respondent has given Apple a technical capability notice?

34. The submissions were, understandably, advanced by reference to the NCND policy. However, as Mr Beard noted, the underlying issue for the Tribunal is what is required to secure open justice so far as consistent with rule 7 of the Tribunal's rules. That in turn requires the Tribunal to decide if it would be

damaging to national security to reveal whether the respondent has given Apple a technical capability notice. If so, then any part of the substantive hearing which would tend to reveal that fact cannot be heard in public.

35. The Tribunal has already decided that it would not be damaging to national security to reveal the fact of these proceedings, the parties to the proceedings and the fact that it concerns the respondent's powers to give a technical capability notice to a relevant operator. There was extensive media coverage both before and after that decision to the effect that a technical capability notice had been given. That coverage was consistent with public statements made by the US Director of Intelligence and with statements attributed to the President of the USA. It was also consistent with what, if the media coverage is taken at face value, were private media briefings provided by Government officials. There is no evidence that any of this is assessed to have damaged national security.

36. Further, the evidence shows that the Government has not consistently applied NCND in this context. First, two different reputable newspapers have reported that Government officials departed from NCND and positively confirmed the existence of a technical capability notice. Journalists protect their sources and sometimes describe them in terms that are not entirely precise (and on occasion not entirely accurate). Some care therefore needs to be taken before assuming the truth of the content of a newspaper article. However, it is difficult to see any source protection reason why The Times and The Financial Times should have described their sources as Government officials if they were not either a member of the Government or a civil servant or special adviser. Notwithstanding what

is asserted at paragraph 15 of Mr Scurry's statement, Mr Sheldon did not submit that we should find the reporting to be untruthful or materially misleading.

37. The assertion that investigations did not reveal a Government source has little or no evidential value in the absence of any further detail about what the investigations involved: see, by analogy, *Attorney General v BBC* [2022] EWHC 380 (QB) *per* Chamberlain J at [30]-[31].

38. Moreover, we infer that it is extremely unlikely that multiple Government sources would have briefed the media in the absence of authorisation for such briefing. Otherwise, the sources would have exposed themselves to the jeopardy of disciplinary and criminal proceedings for no evident personal gain. Conversely, there is nothing inherently unlikely about a scenario in which Government formally maintains NCND in the face of media inquiries (to seek to preserve the integrity of its NCND policy and its litigation stance) whilst at the same time informally departing from NCND by providing briefings to journalists (to provide a narrative that might have political or diplomatic benefit).

39. Importantly, it was open to the respondent to file detailed evidence on this issue. She has chosen not to do so. We were told that it is not usual practice for a Government Security Group investigation to be disclosed, even to the sponsoring department. That is nothing to the point. There is no suggestion that there is any legal impediment to the disclosure to the Tribunal (in CLOSED if necessary) of the relevant investigation reports. In any event, it was open to the

respondent to file direct evidence from Ministers or senior officials that the media briefings were unauthorised. Again, she has chosen not to do so.

40. In all the circumstances, we infer that the briefings that are reported by The Times and The Financial Times did take place, and that they were authorised by Government Ministers or senior department officials or special advisers. This amounts to a significant departure from NCND.

41. There are, additionally, the briefings of members of the US executive and legislature. The fact that the UK Government has confidentially briefed a foreign intelligence liaison partner will not generally undermine its NCND stance. This is because, ordinarily, intelligence partners respect confidences. Here, however, it was abundantly clear by April 2025 that the most senior US officials and politicians were not prepared to keep secret what they regarded as an egregious breach of the First Amendment rights of US citizens. In that context, the respondent's decision to authorise Apple to conduct further briefings of members of the US executive, without any apparent assurance of confidentiality, amounted to a further clear departure from NCND.

42. The cumulative effect of these departures from NCND is that anyone with even a passing interest in this topic already knows that the respondent has served a technical capability notice on Apple. We use the word "knows" advisedly. We accept that in some contexts there may be a real difference between strongly suspecting something on the basis of credible reporting and knowing it on the basis of specific confirmation by a Government source. In this context, where (as we find) authorised confirmations have been given to reputable newspapers

and to foreign officials and legislators who do not regard themselves as bound by any duty of confidence on the subject, it is in our view a distinction without a difference. We have also borne carefully in mind that any assessment of the national security impact of confirming a particular fact must take account of the range of capability of malign actors. Some, including some adversary states, will be sophisticated. Others, such as those who may be contemplating lower level terrorist or criminal activity, may be much less well-informed. We have no doubt that confirmation of the fact at issue here would supply those in the first category with no information whatsoever that they do not already have. We are also satisfied that anyone in the second category who is remotely interested in discovering whether a technical capability notice had been served on Apple could already find the answer to that question with ease. We were told, for example, that an affirmative answer, backed by reference to the press reporting we have discussed, can be found by simply typing the question into Google's chatbot. On the facts of this case, the suggestion that official confirmation would add materially to the stock of information available to a unsophisticated malign actor seems to us to be fanciful.

43. All that being the case, we do not give any significant weight to the respondent's assessment that it would be damaging to national security publicly to depart from NCND, in these proceedings, on the question of whether she has given Apple a technical capability notice. We have carefully considered the evidence that is relied on by the respondent in support of that assertion, including the evidence served in CLOSED. Given that which is already in the public domain, and the extensive (but unacknowledged) departures from NCND that have

already taken place, none of that evidence provides convincing support for the respondent's assertion. We consider the assessment contained in that evidence to be flawed in the public law sense because it fails to take into account or properly grapple with a critical material consideration: the extensive—and on our findings authorised—departures from NCND.

44. Accordingly, we agree with the NGOs and with Apple that the respondent has not established that it would be damaging to national security to reveal in these proceedings, as is the case, that the respondent has given Apple a technical capability notice. It follows that any part of the substantive hearing in these proceedings which involves such confirmation can properly take place in OPEN unless there is some separate basis for requiring secrecy to prevent damage to national security or the broader public interest.

Practical impact of allowing the existence of a technical capability notice to be disclosed during the OPEN proceedings

45. The practical consequence of recognising that it is not damaging to the public interest to disclose the existence of a technical capability notice is that much of the substantive hearing in these claims can take place in OPEN.

46. Apple has five grounds of challenge. The first two concern whether the respondent has power to issue warrants for targeted interception of communications outside the United Kingdom, and whether the statutory power can be used to regulate the security or privacy services offered by a technology company to its customers. These are questions of statutory interpretation that do not depend on evidence. They can be determined entirely in OPEN. The third

ground concerns the consultation process. It is likely that the substance of that ground can also largely be determined in OPEN.

47. The fourth ground concerns whether the technical capability notice amounts to a disproportionate interference with qualified rights under the European Convention on Human Rights. That will require an assessment of whether four tests are satisfied: *Bank Mellat v Her Majesty's Treasury (No 2)* [2013] UKSC 39; [2014] AC 700 *per* Lord Reed at [74]. Those tests are (1) whether the objective of the measure is sufficiently important to justify the limitation of a protected right, (2) whether the measure is rationally connected to the objective, (3) whether a less intrusive measure could have been used without unacceptably compromising the achievement of the objective, and (4) whether, balancing the severity of the measure's effects on the rights of the persons to whom it applies against the importance of the objective, the former outweighs the latter. It is likely that the first three of those tests can largely be determined in OPEN. We do not prejudge where the precise dividing line should fall between that which can be published without damaging the public interest. On any view, however, it is likely that the determination of the fourth test may involve the consideration of evidence that would be damaging to the public interest.

48. The fifth ground concerns whether Apple has been treated differently from other technology companies. Again, it is likely that will involve consideration of evidence that cannot be disclosed in OPEN.

49. It follows that revelation of the fact that there is a technical capability notice allows much (but not all) of the substance of these claims to be determined following public hearings conducted in OPEN.

Disclosure of the detail of the technical capability notice

50. The disclosure of the detail of the technical capability notice is another matter. Although there has been extensive media coverage and public statements about the existence of a technical capability notice, there has been no publication of its precise content. All parties recognise that there may be matters of detail that must be kept secret in order to preserve national security and the public interest. We agree that it would be damaging to national security if all of the material (including the content of the technical capability evidence, and the evidence of Apple and the respondent) were publicly disclosed. That does not mean every detail must be kept secret in order to preserve national security. There may be some information that could be disclosed publicly without damaging national security. It is not, however, practical to determine the precise boundaries now. That is because the key issue for the Tribunal is the extent to which the open justice principle requires public disclosure, so far as that can be secured without damaging national security. The resolution of that issue requires a close analysis of what relevant evidence and arguments the parties will seek to deploy at the substantive hearing. We have already observed that it may be possible to determine the first two grounds of claim entirely in OPEN. If so, it may not be necessary to confront the question of whether disclosure of some details that are not relevant to those grounds would be damaging to national security. It is also likely that parts of the remaining grounds will, in any event, have to be

considered in PRIVATE and CLOSED. It will only be after the parties have exchanged their evidence and written arguments that it will be possible to draw dividing lines as to what evidence is truly relevant to each issue, what is truly damaging to national security, and where the OPEN/PRIVATE/CLOSED boundaries should lie. There is also the possibility that some parts of the hearing could be litigated on the basis of assumed facts, or on the basis of highly generalised gists of the actual facts. Again, that cannot sensibly be determined now.

Outcome

51. We reject the respondent's contention that it would be damaging to national security to confirm the fact that the respondent has given Apple a technical capability notice. The extent, if at all, to which some of the detail of the technical capability notice may be disclosed without damaging national security or the public interest is better addressed separately, after disclosure of evidence and when the precise issues to be determined at the hearing are clear.