



Neutral Citation Number: [2025] UKIPTrib 7

IPT/19/175/CH

IN THE INVESTIGATORY POWERS TRIBUNAL

24 June 2025

Between

NYP

Claimant

-and-

(1) NATIONAL CRIME AGENCY

(2) GREATER MANCHESTER POLICE

Respondents

Introduction

1. This is the judgment of the Tribunal, consisting of Lord Boyd of Duncansby, Vice-President and Ms Darlow KC.
2. The claimant has brought proceedings under section 65(2)(a) of the Regulation of Investigatory Powers Act 2000 ('RIPA') and made a complaint under section 65(2)(b) of the same Act. The claimant's case is that he was unlawfully arrested following his wrongful identification as a suspect in an investigation into the uploading of an indecent image of a child. The proceedings and complaint raise allegations that the National Crime Agency ('NCA') and the Greater Manchester Police ('GMP') were responsible for a breach of his human rights under the European Convention on Human Rights ('ECHR'), and in particular Article 5 and Article 8.
3. The alleged breaches arise from the arrest on 20 April 2018 of the claimant by officers of the GMP. The claimant's arrest followed the receipt of information by the NCA from an

organisation based in the United States, which purported to show that the user of a Microsoft OneDrive account had uploaded an indecent image of a child using an internet protocol ('IP') address.

4. The information relating to the upload was submitted on 3 January 2018 by the NCA to the GMP, in the form of an intelligence report. Having received the NCA report, the GMP made an application under RIPA for communications data, to identify the person associated with the IP address disclosed in the report.
5. The response to the RIPA application suggested that, at the time of the upload of the indecent image, the IP address was registered to the claimant. A second RIPA application was made by the GMP, to ascertain whether the Microsoft OneDrive account disclosed in the report was linked to the claimant or to another individual. However, on 20 April 2018, before a response to this application was received, GMP arrested the claimant. Further RIPA applications were made by GMP; each of which post-dated the arrest of the claimant.
6. The investigation into the claimant by GMP was discontinued on or about 13 July 2018, without any charges having been brought. Nevertheless, the impact of the arrest and the subsequent investigation on the claimant was considerable and enduring. NYP is a father and grandfather and social services were notified of the suspicions of GMP, with distressing consequences which were disruptive of NYP's family life.
7. There is no suggestion on the part of either the NCA or the GMP that the claimant is guilty of any wrongdoing and the Tribunal proceeds on the basis that the claimant is entirely innocent of these matters.
8. There has been no public hearing in this case; however the Tribunal has had the considerable benefit of written submissions from Mr William Hays, who was appointed as Counsel to the Tribunal ('CTT') and from each of the two respondents. The Tribunal has also had the benefit of considering the contents of the claim form and the complaint form; an e-mail from the claimant dated 3 October 2022 and a five-page document from the claimant in support of the claim and complaint forms.
9. Since there has been no public hearing and the claimant was never charged with any criminal offence, the Tribunal acknowledges that the claimant's legitimate expectation of privacy under Article 8 of the ECHR has been engaged. The Tribunal has therefore decided that it would be right to anonymise the claimant for the purposes of this judgement, in which he will be referred to as "NYP".

Procedural History

10. The claim and complaint were both submitted to the Tribunal on 17 September 2019. Following a direction by the Tribunal that the respondents disclose material to the claimant, NYP was notified by the Tribunal that it proposed to proceed by way of receipt of written submissions from the claimant, respondents and CTT, affording the claimant and respondents a right to reply to submissions by CTT, and for the Tribunal thereafter to consider the material and submissions and make a decision without an oral hearing. The claimant agreed with the proposal to proceed without an oral hearing.

11. On 21 December 2023, the Tribunal proposed a formulation of the issues between the parties and provided an opportunity for the parties to respond. Following submissions, the Tribunal agreed the following final formulation of the issues by Order dated 22 May 2024:

1. *Whether the Tribunal has jurisdiction to consider the complaint/claim as against the First and/or Second Respondents given (as the Second Respondent puts it) “the origin of the data to which it relates.”*
2. *Whether the First and/or Second Respondent, in their use of the data relating to username 1829582040048519 which was sent to the Second Respondent by the First Respondent on 18.1.18¹, breached the Claimant’s rights under Article 5 and/or Article 8 of the European Convention on Human Rights.*
3. *If so, the appropriate remedy.*

12. On 8 August 2024, NYP was offered the opportunity to present further submissions in writing. He indicated on the same day that he had no submissions additional to those already provided.

Factual Background

13. On 22 December 2017, the NCA received a ‘Cyber Tipline’ report 26294231 from a private non-profit organisation based in the United States; the Centre for Missing and Exploited Children (‘NCMEC’). The information contained within the Cyber Tipline report had originally been submitted to NCMEC by Microsoft Online Operations. The report detailed that a Microsoft OneDrive username *****519 (‘519’) had uploaded an indecent image of a child via the OneDrive account using an IP address, *.*.115.91 (‘the 115.91 IP address’) at 11:23:34 UTC on ‘7/12/2017’. The date format used is stated in the Report to be in the North American format of month/day/year.

14. An IP must be used in order to browse the internet via broadband. Individual IP addresses are allocated by the customer’s Internet Service Provider. IP addresses may be moved between customers by the Internet Services Providers as and when required.

15. The Cyber Tipline report was reviewed by the NCA Child Sexual Exploitation Referrals Bureau (‘CSE RB’.) At that stage, the identity of the user of the 115.91 IP address was unknown. The NCA used open-source research to verify that the relevant telecommunications operator was British Telecom (‘BT’) and identified the geo-location of the IP address, which corresponded to a named area in the north-west of the United Kingdom. The indecent image was assessed to be Category C, in line with the Sentencing Council Guidelines for the grading of abusive images of children.

16. The Child Exploitation and Online Protection Command (‘CEOP’) of the NCA identified the GMP as the force area corresponding to the geo-location of the IP address and sent an intelligence report to GMP on 3 January 2018, together with a package of other documents, including the Cyber Tipline report and an encrypted disc containing the indecent image.

¹ The date may be an error; the information appears to have been sent on 3.1.18

The intelligence report indicated that the NCA had not carried out any other research on either the subject or the location and stated that the receiving police force should conduct its own local enquiries as necessary to progress the matter. Included in the report was the following: *‘Intelligence disseminated to Greater Manchester Police for information and consideration for any action deemed necessary.’*

17. GMP commenced a criminal investigation. Between 3 January 2018 and 1 July 2018, five applications seeking communications data pursuant to section 22(2) of Chapter II of Part I of RIPA², were submitted by the GMP. In each instance, the type of data sought was ‘traffic data’.
18. The first RIPA application 176490 was made on 3 January 2018. The application sought the identity of the IP address which had uploaded the indecent image at the date and time specified in the intelligence received from the NCA, having transposed the date from the North American format to the United Kingdom format of day/month/year. The purpose of this application was to identify the address, name and contact details of the person believed to have uploaded the indecent image. The obtaining of the data was stated to be necessary on the basis that it would ‘identify the suspect/offender in this crime’ and lead to a further warrant to seize items capable of uploading and storing data to OneDrive Microsoft peer to peer software. It was said to be proportionate on a similar basis and that once the information was known, a warrant could be obtained to seize evidentially relevant items and apprehend and identify the offender.
19. The response from PlusNet, which was received by GMP on 5 January 2018, disclosed the information that the claimant was the user of the IP address 115.91 at the relevant date and time.
20. The second application 80775 was made on 28 February 2018. This application sought information as to whether the Microsoft OneDrive account 519 was associated to the claimant or to someone else, in the one day period prior to the date of the application. The underlying purpose of the application was to seek corroboration of the identification of the user of the IP address.
21. On 20 April 2018, before a response was received to the second application, NYP was arrested by GMP on suspicion of downloading and distributing indecent images of a child. His internet-enabled devices were seized, he was interviewed under caution and strenuously denied the allegations. NYP was then released on bail pending further investigations.
22. On 25 April 2018, five days after the claimant’s arrest, the response to the second RIPA application was received by GMP, which identified a second individual, who may be referred to for the purposes of this judgment as ‘Person X’, as the user of the Microsoft Account. Person X was designated as a second suspect by GMP.
23. Person X lived near NYP and was also a PlusNet customer. The investigation disclosed no evidence of any kind that Person X was known to, or connected with, the claimant. Person X was arrested on 28 April 2018 and his devices were seized and later interrogated but

^{2 2} Part 1, Chapter II of RIPA was subsequently repealed by Schedule 2 of the Investigatory Powers Act 2016 (‘the IPA’) and its provisions replaced by new provisions in Part 3 of IPA.

disclosed no incriminating evidence. In interview he denied any wrongdoing but confirmed that he was the user of the Microsoft OneDrive account 519; albeit averring that his usage of the account ceased in December 2017.

24. On 30 April 2018, a third application 184797 was made, the purpose of which was to seek the IP login history and first registration login history for the Microsoft OneDrive 519, over a date range extending to the period a week before and a week after the believed date of the download of the image. The relevance of the information sought was stated to be 'to either eliminate or implicate' the claimant or Person X. However, the response from Microsoft indicated that the data sought no longer existed, the data retention period being one of ninety days.
25. Additional checks were made by the police with BT (the owners of PlusNet), who confirmed on 6 June 2018 that the claimant had been accurately identified as the user of the 115.91 IP address. GMP further requested, on 8 June 2018, that the content of the Cyber Tipline report be checked.
26. The fourth application, 187584, was made on 14 June 2018. The purpose of this application was to establish whether the 115.91 IP address had been allocated to the address linked to Person X during any time over a specified period of approximately six months, which included the believed date of the download. This extended date period allowed for the possibility that the date of the download supplied in the Cyber Tipline report had been misinterpreted as a result of confusion over the style of date format and the day and month had been erroneously reversed. Had this occurred, the longer date period would have enabled the identification or elimination of the error. The ensuing response from PlusNet sought clarification as to the precise address, since the premises identified in the application were divided into nine flats.
27. The fifth and final RIPA application, 188700, was made on 1 July 2018 and again sought information as to the allocation of the 115.91 IP address to the address linked to Person X, specifying that each of the nine flats should be included within the request. In response, PlusNet indicated that the relevant IP address had been allocated to one of the relevant addresses for a single, short interval of time. This period fell within the period specified in the application but did not coincide with the date and time of the relevant download.
28. The information derived from the five applications thus indicated, in summary, that the IP address 115.91 was allocated to the claimant at the time and date on which the download was believed to have been made, but the Microsoft OneDrive account used to upload the image was registered to Person X. Person X, although unconnected to the claimant, had also been allocated the relevant IP address, albeit for a different date period which did not overlap with the time and date of the upload. The overall evidential picture thus disclosed substantial inconsistencies and provided strong support for the inference that one or more serious errors had occurred, without necessarily clarifying precisely the nature of those errors.
29. The source of the inaccurate information as to the claimant's IP address was therefore the NCA, who supplied the information to GMP, who acted upon the information.
30. The origin of the error leading to the identification of NYP as the user responsible for the upload has never been conclusively identified, although a number of potential hypotheses

have been suggested. The error would be of potential relevance if the available evidence indicated that it was, or might be, attributable to the deliberate or reckless actions of either of the respondents. Given the observation of the Tribunal above that NYP is innocent of the allegations, the Tribunal does not propose otherwise to engage in a speculative determination as to the potential source of the error.

31. On or about 13 July 2018, the investigation against the claimant was concluded with no further action being taken and his property was restored to his possession. The claimant states that he was informed by the investigating officer that he was ‘totally innocent’ and it was intimated to him that the responsibility for his arrest lay with PlusNet.
32. A ‘serious error’ report was made by GMP to the Investigatory Powers Commissioner on 3 September 2018 and an investigation was commenced. As part of the investigation, BT were requested to check and re-run the disclosure provided in response to the five RIPA applications; this confirmed that the disclosures made were correct. NCMEC were contacted through the NCA and requested to recheck and verify the original Cyber Tipline report. NCMEC responded by advising that Microsoft, as the original source of the information, should be contacted. This was duly done and Microsoft’s response indicated they had no reason to doubt the accuracy of the information.
33. Legal representatives acting on behalf of the claimant subsequently made a claim against PlusNet and the claimant has provided to the Tribunal copies of correspondence with BT in March and April of 2019. Within this correspondence, BT affirmed the accuracy of its response to the RIPA requests and indicated that the information provided in response, including the authentication of the 115.91 IP address, was re-checked on 26 February 2019 and no error was identified. BT also provided the information that the IP address was a ‘Dynamic IP Address’; namely a temporary address assigned to a computing device when it is connected to the network, which can then be reallocated to a different customer when the first user leaves the network. BT noted that for this reason, it is essential that the data and time of interest are accurately identified in a RIPA request.

Material Legislation

The Acquisition of Communications Data

34. At the time of the relevant authorisations, the acquisition of communications data was governed by Chapter II Part I of RIPA, to which the Acquisition and Disclosure of Communications Code of Practice relates (‘the Code of Practice’). Each of the five applications was made under the provisions of section 22 of Chapter II of RIPA.
35. The meaning of communications data, as defined in section 21(4) of RIPA, includes traffic data comprised in or attached to a communication for the purpose of any postal service or telecommunication system by which it is transmitted. Traffic data, as defined in section 21(6) of RIPA, may include IP address allocation.³

³ See Codes of Practice, para 2.26.

36. Section 22 of RIPA ⁴ applies where a designated person believes that it is necessary, on one of the grounds falling within section 22(2), to obtain any communications data. A designated person is someone holding a prescribed office, rank or position within a relevant public authority that has been designated for the purpose of acquiring communications data by order. Police forces are included as relevant public authorities.⁵
37. The grounds falling within subsection (2) include that the obtaining is necessary for the ‘applicable crime purpose’.⁶ In so far as material, ‘the applicable crime purpose’ means the prevention and detection of serious crime, which includes an offence carrying a term of imprisonment of 12 months or more.⁷ The offences of possession and distribution of indecent photographs of children both fulfil the definition of serious crime.
38. The designated person shall not grant an authorisation unless he believes that obtaining the data in question is proportionate to what is sought to be achieved by obtaining the data. Where this is so, the designated person is then authorised to require the telecommunications operator to disclose the data sought. The Code of Practice states that proportionality involves balancing the extent of the interference with an individual’s rights and freedoms against a specific benefit to the investigation.⁸

The Jurisdiction of the Investigatory Powers Tribunal

39. The Investigatory Powers Tribunal was established by RIPA, pursuant to which it holds jurisdiction to consider two types of cases, human rights actions and complaints. RIPA has been subject to a number of revisions subsequent to the dates of the relevant conduct, namely the period between December 2017 and August 2018. The analysis which follows will therefore refer to the version of RIPA then in force.⁹
40. Section 65(2)(a) of RIPA provides that the Tribunal shall be, ‘*the only appropriate tribunal for the purposes of section 7 of the Human Rights Act 1998 (‘HRA’) in relation to any proceedings under subsection (1)(a) of that section (proceedings incompatible with Convention rights) which fall within subsection (3) of this section.*’
41. Proceedings falling within section 65(3)(d) of RIPA include ‘*proceedings relating to the taking place in any challengeable circumstances of any conduct falling within subsection (5).*’
42. As to the first of the two requirements, section 65(7) of RIPA provides, as is material, that conduct takes place in *challengeable circumstances* if it takes place with the authority, or purported authority, of anything falling within subsection (8); or the circumstances are such that (whether or not there is such authority) it would not have been appropriate for the conduct to take place without it, or at least without proper consideration having been given to whether such authority should be sought.

⁴ In the version in force at the relevant time.

⁵ ‘Police force’ is defined in section 81(1) of RIPA.

⁶ Section 22(2)(b).

⁷ See section 25(1) of RIPA.

⁸ At paragraph 2.5.

⁹ The statutory basis for the Tribunal’s retained jurisdiction derives from section 16 of the Interpretation Act 1978.

43. Conduct falling within subsection (8) includes, by virtue of subsection 8(b), an authorisation or notice under Chapter II of Part 1 of RIPA. Chapter II of RIPA governs the acquisition and disclosure of communications data.
44. As to the second requirement, *conduct falling within subsection (5) of RIPA includes 'conduct to which Chapter II of Part I applies' (by section 65(5)(c)).*
45. Section 65(2)(b) of RIPA provides that the jurisdiction of the Tribunal shall be, *'to consider and determine any complaints made to them which, in accordance with subsection (4) are complaints for which the Tribunal is the appropriate forum.'*
46. Subsection (4) provides that:
- The Tribunal is the appropriate forum for any complaint if it is a complaint by a person aggrieved by any conduct falling within subsection (5) which he believes –*
(a) to have taken place in relation to him, to any of his property, to any communications sent by or to him, or intended for him, or to his use of any postal service, telecommunications service or telecommunications system; and
(b) to have taken place in challengeable circumstances or to have been carried out by or on behalf of any of the intelligence services.
47. As discussed above, subsection (5) includes conduct to which Chapter II of Part I applies, namely the acquisition of communications data. Challengeable circumstances would include conduct taking place in accordance with an authorisation or purported authorisation for communications data under Chapter II of Part 1.

The European Convention on Human Rights

48. Article 5 of the ECHR, in so far as material, provides:

(1) Everyone has the right to liberty and security of person. No one shall be deprived of his liberty save in the following cases and in accordance with a procedure prescribed by law:

...

(c) the lawful arrest or detention of a person effected for the purpose of bringing him before the competent legal authority on reasonable suspicion of having committed an offence ...

...

(4) Everyone who is deprived of his liberty by arrest or detention shall be entitled to take proceedings by which the lawfulness of his detention shall be decided speedily by a court and his release ordered if the detention is not lawful.

(5) Everyone who has been the victim of arrest or detention in contravention of the provisions of this Article shall have an enforceable right to compensation.

42. Article 8 ECHR provides:

1. Everyone has the right to respect for his private and family life, his home and his correspondence.

2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

The Claimant's Submissions

49. The case of the claimant, who was not legally represented for the purposes of these proceedings, has been set out in the claim and complaint form and supporting documents. He asserts that his rights under Article 5 and Article 8 have been breached. The claimant states that he was wrongly identified as a suspect, unlawfully arrested, detained in police custody and interviewed. The consequent involvement of social services resulted in his loss of unsupervised contact with his grandchildren. He faced the stigma of arrest on suspicion of an offence viewed with revulsion by wider society. The information provided to him by GMP, when he was informed that the investigation against him was at an end, indicated that GMP had relied on false information provided by PlusNet, upon which GMP placed undue reliance.

50. Upon a point of evidence, the claimant further points out a discrepancy between the approximate geo-location of the IP address identified by the NCA, which he has never visited, and his own address. The Tribunal notes that whilst both are in the geographical region, they are not contiguous.

Submissions on behalf of Counsel to the Tribunal

Issue One

51. So far as Issue One is concerned, CTT submits that the role of the NCA was limited and essentially consisted of transmitting information which it had received from NCMEC to GMP, having made an assessment of that material. Their role in transmitting this information fell outside the conduct to which Chapter II of Part I of RIPA applies. The regulatory framework of RIPA is concerned with the 'obtaining' of data by public authorities and the 'disclosure' of data by the telecommunications operator. It is not concerned with the onward disclosure of data that had previously been obtained by a public authority from a telecommunications operator.

52. CTT therefore supports the submissions of the NCA that its conduct falls outside the jurisdiction of the Tribunal.

Issue Two

53. In summary, CTT supports the contention of the GMP that the Tribunal has no jurisdiction to consider the legality of NYP's arrest or the consequences upon NYP of the arrest and investigation.
54. Considering the jurisdiction of the Tribunal in respect of a complaint for false arrest, CTT suggests that the claimant would need to contend that the conduct, namely the arrest, was conduct to which Chapter II of Part I of RIPA applies and that the conduct took place in challengeable circumstances because it was conduct which required authorisation under Chapter II. This would be a difficult argument to advance, since the arrest of a person is not conduct to which Chapter II applies, nor does it require authorisation under Chapter II.
55. Similar considerations apply in respect of the Tribunal's jurisdiction to consider a human rights action for wrongful arrest. Mr Hays has analysed with care the points that might be advanced on behalf of the claimant. He suggests that the claimant might wish to contend that the proceedings for a breach of Article 5 are '*proceedings relating to*'¹⁰ the obtaining of communications data, on the grounds that the arrest was solely based upon the communications data thereby obtained. However, this contention would involve an expansion of the Tribunal's jurisdiction in reliance upon the undefined term '*relating to*' which would potentially draw many other decisions by the police into the jurisdiction of the Tribunal, simply on the basis that there is some factual nexus between those decisions and the acquisition of communications data. Further, the contention would imply that the subject matter for which a human rights claim may be brought before the Tribunal is far wider than that upon which a complaint could be brought; a consequence for which there is no apparent rationale.
56. The acquisition of communications data falls squarely within the jurisdiction of the Tribunal. In assessing whether the decision of GMP involved a breach of Article 8, CTT suggests that the Tribunal may wish to afford a measure of respect to the balance of rights and interests struck by the GMP (*Dalston Projects Limited, Sergei Georgievich Naumenko, Prism Maritime Limited v Secretary of State for Transport* (2024) EWCA Civ 172, per Singh LJ at [11] to [21]).
57. GMP have relied upon the contention that the obtaining of communications data was necessary and proportionate. CTT submits that there could be cases where an entity obtains communications data either knowing, or being reckless, as to whether the information sought, does not relate to a person who might be suspected of a criminal offence. However, on the facts of this case, CTT concludes that such a scenario does not apply; Microsoft have confirmed that the information provided is correct.

¹⁰ Within the meaning of section 65(3)(d).

Submissions on behalf of the Respondents

Issue One

58. The NCA emphasises that its role was limited to the receipt of information from NCMEC and the dissemination of this information to the GMP. The first respondent relies upon the statutory limitations to the jurisdiction of the Tribunal over the claim and complaint and disputes that any of its conduct fell within the jurisdiction of the Tribunal as provided by section 65 RIPA. The relevant conduct met neither of the two limbs of the test required for the Tribunal to have jurisdiction; it neither fell within section 65(5), nor was it conduct which took place in challengeable circumstances.
59. The wide range of conduct falling within section 65(5) does not include the receipt of information from a third party, nor its dissemination to a further third party. Considering section 65(5), of the two provisions of that subsection which might arguably be capable of applying to this case, section 65(5)(ba) concerns ‘*conduct for or in connection with the obtaining of secondary data from communications transmitted by means of (a postal service or telecommunications system).*’ The NCA contends that the unsolicited receipt and use of such data cannot properly fall within the meaning of ‘*obtaining of secondary data*’ without stretching the definition of ‘*for or in connection with*’ to its breaking point.
60. The second provision identified by the NCA as of potential relevance is section 65(5)(c), which refers to conduct of a kind which may be permitted or required by an authorisation or notice under Part III of the Investigatory Powers Act 2016 (‘IPA’). The territorial extent of the IPA, as provided by section 272(4) IPA, does not include the USA. It will be apprehended however, that this reference (as indeed is the previous subsection referred to by the NCA) is to a version of section 65 of RIPA not in force at the relevant time. The version of subsection (5)(c) relevant to this determination is cited earlier in this judgment.
61. The NCA disputes that the jurisdiction of the Tribunal extends to determining any tortious claim; a wrongful arrest or false imprisonment claim is a claim in tort at common law.
62. On behalf of the GMP, no jurisdictional point is taken in relation to Issue One.

Issue Two

63. On behalf of the NCA, it is emphasised that the agency played no role in the arrest of the claimant and its involvement in the matter ceased on 3 January 2018. The first respondent contends that in the circumstances of this case, liability for an Article 5 breach should not properly be considered to extend beyond the detaining agency, distinguishing *Zenati v Commissioner of Police of the Metropolis* [2015] EWCA Civ 80.
64. Whilst acknowledging that Article 8 is engaged by the receipt, processing and dissemination of information about an individual, the NCA submits that its receipt and dissemination of information about the possession by an individual of an indecent image of a child fall within the conditions under Article 8(2), under which a public authority may interfere with the rights protected by Article 8(1).

65. The receipt of information was '*in accordance with the law*'; the NCA has a power to receive and disclose information in connection with the exercise of its function: section 7 of the Crime and Courts Act 2013. The functions of the NCA include disseminating information relevant to activities to combat any kind of crime, under section 1(4) of that Act. The dissemination of the information was '*for the prevention of disorder or crime*' and '*for the protection of the rights and freedoms of others*'. It would have been unconscionable for the NCA not to have acted on that information. The dissemination was both necessary and proportionate.
66. The GMP deny acting unlawfully at any stage. The RIPA applications were authorised and managed in accordance with the legislation. The error in relation to the IP address and the Microsoft OneDrive account was not one of GMP's making and the reasons for the error remain unclear.
67. The role of GMP was to receive intelligence from the NCA and thereafter to investigate, which included the exercise of its powers under section 22 of RIPA to obtain the name of the customer to whom the IP address was allocated. Following receipt of information that the claimant was the user of the IP, GMP attempted to corroborate that information by obtaining additional information from Microsoft and when such corroboration was not received within a reasonable time, proceeded with the arrest of the claimant and continued to make further requests to ascertain the identity of the offender. The reasonableness of the time period should be viewed in the context of an ongoing investigation into a serious offence presenting a potential ongoing risk of harm to children.
68. The use of data received by GMP from the NCA was necessary and proportionate and thus lawful under Article 8 of the ECHR and there was an overwhelming public interest in identifying the offender. The RIPA applications and authorisations demonstrate that full consideration was given to the issues of necessity and proportionality.
69. GMP also disputes that the Tribunal has jurisdiction to adjudicate upon the lawfulness of the claimant's arrest, including whether the arrest complied with Article 5. The jurisdiction of the Tribunal in this case is confined under section 65(5)(ba) of RIPA. The arrest of the claimant was not conduct capable of falling within such a definition; it falls under, and is regulated by, the Police and Criminal Evidence Act 1984 ('PACE') and is under the jurisdiction of the civil courts.
70. In any event, the arrest was lawful because it was based upon a reasonable suspicion and was necessary for the prompt and effective investigation of the offence. Corroboration prior to arrest had been sought, but not received.

Discussion and Decision

71. The Tribunal accepts the claimant's account that his arrest was highly distressing; events were witnessed by some of his neighbours and he was later held in a police cell. Following a safeguarding meeting, restrictions were placed on the claimant's contact with his grandchildren and for approximately one year after his arrest, he lived with his daughter. The arrest and the subsequent investigation had a profound and damaging impact upon his life, mental health and general wellbeing.

Issue One: whether the Tribunal has jurisdiction to consider the complaint/claim given the ‘origin of the data’

72. GMP does not contest that the complaint and claim, in so far as the applications for communications data are concerned, falls within the jurisdiction of the Tribunal, a concession rightly made. In so far as the NCA are concerned, the Tribunal must consider whether the unsolicited receipt of data from an overseas body and/or subsequent onward dissemination of the data, is capable of constituting ‘conduct’ falling within section 65(5) of RIPA.
73. Section 65(5) covers a range of conduct including surveillance, the interception of communications, the giving of a notice under section 49 and entry on, or interference with, property. Such conduct is regulated by RIPA, the IPA and the Police Act 1997 and is of the type to require authorisation and/or warrant and oversight under the regulatory framework. Neither the receipt by the NCA of information from the NCMEC, nor the dissemination of this information, can properly be said to fall within any of the provisions of section 65(5).
74. The acquisition and disclosure of communications data under section 22 of RIPA falls within section 65(5)(c) (*‘conduct to which Chapter II of Part I relates’*). Chapter II concerns the obtaining of communications data and its disclosure to any person, which requires authorisation. As section 22(4) of RIPA makes clear, the statutory framework concerns the authorisation of disclosure of information by a *‘postal or telecommunications operator.’* Communications data is described in the Code of Practice as data that is *‘generated, held or obtained in the provision, delivery and maintenance of communications services, those being postal service or communications services.’*¹¹ In the present case, neither the disclosure to the NCA, nor the onward disclosure of, the communications data by the NCA was made by a telecommunications operator; in each case, it was made by a third party. Neither activity therefore constituted conduct which would have required an authorisation under Chapter II of RIPA.
75. On behalf of the NCA, the possibility that the conduct might also fall within section 65(5)(ba) of RIPA was raised for consideration. Section 65(5)(ba) of RIPA was not in force at the relevant time. The subsection relates to the acquisition regime under IPA and in particular, to section 15 (2)(b) of Part II Chapter I of IPA, under which a targeted interception warrant may be issued for the obtaining of secondary data from communications transmitted by means of a postal or telecommunications system. This provision was not brought into force until 31 May 2018 and can thus be of no relevance to the conduct of the NCA which ceased on 3 January 2018, or indeed, to the steps taken by the GMP to obtain information relating to the IP address which had been attributed to the claimant. The applications for communications data in the present case were all made under a statutory regime pre-dating the relevant provisions of the IPA.
76. The actions of NCMEC in receiving the communications data from Microsoft, a telecommunications provider, or of Microsoft in providing the data, both of which took place overseas, also fall outside Chapter II of RIPA. The relevant public authorities who may request communications data are set out in section 25(1), all of which authorities are

¹¹ Code of Practice para 2.16.

within the United Kingdom.¹² They include police forces¹³, the NCA, HM Revenue and Customs and the intelligence services.

77. From this analysis, it must follow that the conduct did not take place in ‘challengeable circumstances’; the conduct of the NCA did not take place with the authority or purported authority of an authorisation or notice under Chapter II of RIPA. Neither may it be said that the circumstances were such that the conduct would not have been appropriate without an authority, or without proper consideration having been given to whether such authority should be sought. It would not have been apparent to the NCA, upon receiving the data from NCMEC, that authorisation under Chapter II was required for the receipt, which was in any event unsolicited. Neither would the onward disclosure of the data to a third party have indicated that authorisation under Chapter II was mandated.
78. Turning to consider the arrest of the claimant, the arrest of a suspect by a police force falls outside the conduct listed in section 65(5)(c) of RIPA, or indeed any other subsection of section 65(5). Neither was the arrest conduct which took place in challengeable circumstances, because it did not require authorisation under Chapter II of Part I of that Act. It cannot therefore fall within the jurisdiction of the Tribunal as provided by section 65(2)(b) of RIPA, to consider and determine a complaint based upon NYP’s arrest, against either respondent.
79. Similar considerations apply to the jurisdiction of the tribunal to determine a human rights claim under section 65(2)(a) of RIPA based upon the arrest of NYP; the conduct neither falls within section 65(5), nor did it take place in challengeable circumstances, for the reasons enumerated above.
80. CTT has suggested, without lending his support to the argument, that a potential submission might be available to the claimant that the Tribunal was ‘*the appropriate tribunal*’ to determine such a claim based upon the wording of section 65(3)(d) of RIPA; (*‘proceedings relating to the taking place in any challengeable circumstances of any conduct falling within subsection (5)’*); namely, that the proceedings arising from the arrest might be said to ‘*relate to*’ the obtaining of communications data.
81. As acknowledged by CTT, such an interpretation would involve an expansion of the jurisdiction of the Tribunal which would draw into its jurisdiction many decisions made by the police, on the sole basis that such decisions ‘relate’ to the obtaining of communications data. The rationale for such an expansion would rest alone upon the use of the word ‘*relating*’ in the relevant subsection. It is apparent from the context that ‘relating’ refers to the proceedings before the Tribunal, rather than decisions or conduct on the part of public authorities which would otherwise fall outside the jurisdiction of the Tribunal, but bearing some factual nexus with conduct within section 65(5). The interpretation suggested would strain the ordinary meaning of the words beyond a point of reasonable tolerance. The wider interpretation would therefore be misconceived.
82. This conclusion is strengthened by the types of conduct deemed to take place in challengeable circumstances under section 65(8), which, in so far as they concern public authorities other than the intelligence services, entirely relate to the Tribunal’s core function

¹² Section 25 RIPA.

¹³ As defined in section 81(1) of RIPA.

in that regard, namely to provide a right of redress to anyone who has been the victim of the unlawful use by public authorities of the intrusive powers of the interception of communications, covert surveillance and other similar powers.

83. Even if this analysis is erroneous, the suggestion interpreted is entirely inconsistent with the restricted statutory footing of the Tribunal. Wrongful arrest is a common law tort and remedies are available in both civil law and potentially criminal law, to those who are victims of unlawful treatment by the police arising from an arrest. As observed by Singh LJ when considering the jurisdiction of the Tribunal in *Al-Hawsawi v Security Service and others* (2023) UKIP Trib 5; ‘*The Tribunal is a creature of statute. It does not have a general jurisdiction, for example to consider or determine civil proceedings. The extent of its jurisdiction is as set out by Parliament in RIPA, no more and no less.*’ [36]. Singh LJ also observed in the same context; ‘*The language used in RIPA does not appear to us to be apt to embrace common law causes of action, in particular claims in tort*’ [44].
84. A decision by the Tribunal that the circumstances of the claimant’s arrest are not within its jurisdiction would not however deprive NYP of a remedy before the civil or criminal courts.
85. Additionally, the powers of arrest, search and seizure are governed by a separate regime, PACE, regulation of which falls outside the jurisdiction of the Tribunal. In *KJF v Surrey Police* (2022) UKIP Trib 7, the Tribunal considered the issue of jurisdiction in respect of the actions of the police in breaking into a mobile phone which had been lawfully seized under a search warrant issued by section 8 of PACE. The Tribunal held that where the seizure of the device had taken place under PACE, even if it subsequently transpired that the seizure was not lawful, the Tribunal had no jurisdiction; ‘*It is a matter for the ordinary courts. This Tribunal has no jurisdiction in respect of PACE powers.*’ [21]
86. In conclusion, the Tribunal holds jurisdiction over the conduct of GMP in seeking communications data under Chapter II of RIPA. It does not hold jurisdiction over the conduct of the NCA in respect of the data, nor over the conduct of either respondent in so far as it concerns the arrest of the claimant.
87. For the sake of completeness, whilst the notification of social services by the police undoubtedly had a grave and upsetting impact on the claimant’s life, the conduct of the police in this regard also falls outside the Tribunal’s jurisdiction.

Issue Two: whether the use of the data by the first and/or second respondent, breached the claimant’s rights under Article 5 and/or Article 8

The approach of the Tribunal

88. In determining a claim or complaint, the Tribunal shall apply the same principles for making their determination as would be applied by a court on an application for judicial review.¹⁴ The principles of judicial review include a review of an administrative decision on the grounds that it was unlawful; the other two grounds of judicial review being procedural impropriety and irrationality.¹⁵

¹⁴ Section 67(2) and (3(c)) of RIPA.

¹⁵ Council of Civil Service Union v Minister for the Civil Service (1985) AC 374 at 410D.

89. Section 6(1) of the HRA makes it unlawful for a public authority to act in a way which is incompatible with the Convention rights, which are set out in schedule 1 of the HRA. In so far as is relevant to the present case, these rights include those in Article 5 and Article 8. Therefore, if the complaint and human rights proceedings succeed in demonstrating unlawfulness, which interfered with the claimant's Convention rights, it will necessarily follow that the interference was not in accordance with the law.
90. Any interference with Convention rights must be '*necessary in a democratic society*' and must satisfy the principle of proportionality. In *Bank Mellat v HM Treasury (No 2)* (2013) UK.SC 39, [2014] AC 700, the test was interpreted as having four limbs. The court or tribunal must ask:
- (i) Whether the objective of the measure is sufficiently important to justify the limitation of the right;
 - (ii) Whether the measure is rationally connected with that objective;
 - (iii) Whether a less intrusive measure could have been used without unacceptably compromising the achievement of that objective; and
 - (iv) Whether, balancing the severity of the measure's effects on the rights of the person to whom it applies against the importance of the objective, to the extent that the measure will contribute to its achievement, the former outweighs the latter (this fourth test is sometimes called the 'fair balance' test or proportionality *stricto sensu*, i.e. in the strict sense.) [20] and [74].
91. In assessing proportionality, the Tribunal must decide that issue for itself, whilst giving appropriate respect and weight to the assessment of the balance of rights and interests struck by a public authority, such as the police (*Director of Public Prosecutions v Ziegler* (2021) UKSC 23, (2022) AC 408 at [130]).
92. The Tribunal considered a claim and complaint involving an allegation that communications data had been unlawfully obtained in *Damian Hill v Metropolitan Police Service & Independent Office for Police Conduct* (IPT/20/62/H). The judgement summarised the relevant principles applicable to section 22 of RIPA at [17]:

"In News Group Newspapers Limited v Commissioner of Police for the Metropolis (IPT/14/176H) the Tribunal considered the operation of section 22 of RIPA and held:

- (a) An applicant for authorisation under RIPA has a duty to include in the application the necessary material to enable the authorising officer to be satisfied that the statutory conditions are met, and must also make full and accurate disclosure, including disclosure of anything that might militate against the grant on an authorisation (para 81, applying Chatwani IPT/15/84/88/CH at para 15).*
- (b) The lawfulness of the authorisation(s) to obtain communications data must be judged on the basis of the information known to the investigation team at the time when the authorisations were issued (para 34).*
- (c) The belief of the designated person as to necessity and proportionality under section 21(1) and (5) must be an honest and reasonable belief (paras 74 and 89)*
and

(d) Whether or not Convention rights have been breached is an objective question which does not depend on the procedural propriety of the decision-making process or the adequacy of the reasoning of the relevant designated person (para 65, applying Belfast City Council v Miss Behavin' Limited (2007) 1 WLR 1420). ”

93. In light of the Tribunal's determination, for the reasons set out above, that the conduct of the NCA in respect of the data and the arrest of the claimant both fall outside the Tribunal's jurisdiction, the remaining relevant use of the data relating to username **519 concerns the RIPA applications made by the second respondent. The fourth and fifth RIPA application concerned Person X and not the claimant, thus the subject matter to be analysed for Issue Two are the first, second and third RIPA applications.
94. The Tribunal has carefully considered the grounds of necessity and proportionality and disclosure duties which must underpin a lawful application of this type and has concluded that each were afforded appropriate consideration by the applicant and were properly and thoroughly set out in each of the three RIPA applications. The investigation was one involving indecent images of children and there was an obvious public interest in pursuing an investigation into offences capable of causing great harm to children. It is difficult to identify a less intrusive measure that might have been deployed to obtain the data than through the making of the RIPA applications, or to determine how otherwise GMP might have progressed an investigation into serious criminality. An appropriate balance was struck between the extent of the interference with the claimant's rights and freedoms and the benefits to the investigation.
95. Each of the applications required the applicant to consider and describe any 'meaningful collateral intrusion.' In the first application 176490, the applicant noted the possibility that the user of the device might be utilising someone else's internet connection, either with or without their consent, but stated that it would not be possible to resolve this possibility prior to obtaining the data; an analysis accepted as reasonable by the Tribunal. A safeguard was offered by the applicant in the eventuality, namely that if the information disclosed this to be the case, the investigation would then be ceased. The risk of collateral intrusion was considered and fairly identified and described. Whilst the response of GMP to the information obtained through the applications, namely the arrest of NYP, was highly intrusive, the applications themselves raised only a low level of collateral intrusion.
96. There is no evidence before the Tribunal that any of the information included by the applicant was inaccurate or materially incomplete, or that the information presented in the applications was relied upon recklessly or in bad faith. The purpose of the application was to identify the individual using the IP address at the time, whilst recognising the inherent risk that the lawful user of the IP address might not be synonymous with the individual who uploaded the image. It is apparent that the data was checked by the GMP during the currency of the investigation. Subsequent rigorous checks of the relevant information, both by BT in response to the claim against PlusNet and during the course of the investigation by the Investigatory Powers Commissioner, has not disclosed any error in the data.
97. It is unclear as to why there was a delay of almost two months between the first and second RIPA application. However, it appears that the investigating officer was concerned that the response to the second application might be delayed, thereby prejudicing the progress of the investigation. In this regard, it may be noted that an e-mail sent to the investigating

officer on 5 September 2018 by another officer raised the issue; ‘we may be asked why he was arrested instead of VA’d¹⁶ and why we didn’t wait for the Microsoft Subscriber to come back beforehand.’ In response, the investigating officer explained that Microsoft ‘took months before getting back, they might never have got back at all. This left us with no option (*sic*) to act against (NYP) in case he was the prime suspect, still committing offences. VA wasn’t the option then as we needed to seize computers etc.’ Whilst this approach may have been reasonable in the circumstances, it may be observed that a more prompt submission of the second application would have afforded more time for Microsoft to respond prior to any decision to arrest the claimant. Nevertheless, the prompt timing of the submissions is primarily an operational function of the police investigation rather than a matter touching upon the lawfulness of the applications themselves.

98. The Tribunal is therefore unable to conclude that the use of the data relating to 519 by either respondent was in breach of the claimant’s Article 5 or 8 rights.

Conclusion

99. For the reasons set out in the judgement, the claim and complaint are both dismissed against each of the respondents.

100. Pursuant to section 67A of RIPA there is a right to apply for leave to appeal this decision. The Tribunal hereby specifies that the relevant appellate court for the purposes of an appeal under section 67 A (2) RIPA is the Court of Appeal of England and Wales.

101. An appeal is possible only in respect of a point of law that raises an important point of principle or practice (or for other compelling reasons) and is not a decision on a procedural matter. An appeal requires permission so an application must first be made to the Tribunal for leave to appeal. A form applying for leave to appeal is attached and full details of the provisions relating to appeal may be found on the Tribunal’s website: www.investigatorypowerstribunal.org.uk.

102. Rule 16 of the Tribunal Rules contains detailed provisions about the making of an application for leave to appeal. The Rules can be found on the Tribunal’s website.

¹⁶ It is assumed this is an acronym for ‘Voluntary Attendance’, denoting a voluntary attendance interview which would have avoided the claimant’s arrest.