Neutral Citation No: [2023] NIKB 60 *Judgment: approved by the court for handing down (subject to editorial corrections)**	*Ref:* **SCO12163** *ICOS No:* **22/030034/01** *Delivered:* **15/05/2023**

IN THE HIGH COURT OF JUSTICE IN NORTHERN IRELAND

_____

KING'S BENCH DIVISION
(JUDICIAL REVIEW)

_____

IN THE MATTER OF AN APPLICATION BY CURTIS TANNER FOR JUDICIAL REVIEW

AND IN THE MATTER OF A DECISION OF THE NORTHERN IRELAND PRISON SERVICE

_____

Dessie Hutton KC and Stephen Toal (instructed by Owen Beattie & Co Solicitors) for the Applicant
Tony McGleenan KC and Terence McCleave (instructed by the Departmental Solicitor's Office) for the proposed Respondent

_____

SCOFFIELD J

Introduction

[1] This challenge relates to the absence of a published policy in respect of when officers of the proposed respondent, the Northern Ireland Prison Service (NIPS), will intercept or monitor prisoners' communications such as telephone calls.

[2] Initially, the application was presented as a challenge to a purported failure on the part of NIPS to formulate a policy or, in the alternative, a failure on the part of NIPS to publish such policy as it had adopted. The proposed respondent then served affidavit evidence, along with various exhibits, which were asserted by it to constitute, or to at least transparently set out, the policy which it applied. Accordingly, the applicant's complaint was reformulated to relate only to the proposed respondent's failure to publish the policy documents which exist.

[3] The case proceeded by way of a rolled-up hearing. Mr Hutton KC appeared with Mr Toal for the applicant; and Mr McGleenan KC appeared with Mr McCleave for the proposed respondent. I am grateful to all counsel for their helpful written and oral submissions.

Rule 68A of the Prison Rules

[4] A key provision in this case is rule 68A of the Prison and Young Offenders Centres Rules (Northern Ireland) 1995 ("the Prison Rules"), which provides as follows:

> "(1) The Department of Justice may give directions to any governor concerning the interception in a prison of any communication to or by any prisoner or class of prisoners if the Department of Justice considers that the directions are –
>
> (a) necessary on the grounds specified in paragraph (4) below; and
>
> (b) proportionate to what is sought to be achieved.
>
> (2) Subject to any directions given by the Department of Justice, the governor may make arrangements for any communication by a prisoner or class of prisoners to be intercepted in a prison by an officer or a person employed in the prison authorised by the governor for the purposes of this rule (referred to in this rule as an "authorised employee") if he considers that the arrangements are –
>
> (a) necessary on any of the grounds specified in paragraph (4) below; and
>
> (b) proportionate to what is sought to be achieved.
>
> (3) Any communication to or by a prisoner may, during the course of its transmission in a prison, be terminated by an officer or an authorised employee if he considers that to terminate the communication is –
>
> (a) necessary on any of the grounds specified in paragraph (4) below; and
>
> (b) proportionate to what is sought to be achieved by the termination.

(4) The grounds referred to in paragraph (1)(a), (2)(a) and (3)(a) above are –

(a) the interests of national security;

(b) the prevention, detection, investigation or prosecution of crime;

(c) the interests of public safety;

(d) securing or maintaining prison security or good order and discipline in prison;

(e) the protection of health and morals;

(f) the protection of the rights and freedom of any person.

(5) Any reference to the grounds specified in paragraph (4) in relation to the interception of a communication by means of a telecommunications system in a prison, or the disclosure or retention of intercepted material from such a communication, shall be taken to be a reference to those grounds with the omission of sub-paragraph (f).

(6) For the purposes of this rule "interception" –

(a) in relation to a communication by means of a telecommunications system, means any action taken in relation to the system or its operation so as to make some or all of the contents of the communication available, while being transmitted, to a person other than the sender or intended recipient of the communication; and the contents of a communication are to be taken to be made available to a person while being transmitted where the contents of the communication, while being transmitted, are diverted or recorded so as to be available to a person subsequently; and

(b) in relation to any written or drawn communication, includes opening, reading, examining and copying the communication."

[5] Rule 67 of the Prison Rules provides the prison authorities with a power to restrict prisoners' communications with those outside prison. This case, however, concerns communications which *are* permitted. Rule 68A, as its title ("Interception of Communications") suggests, is about the monitoring of permitted communications in the course of transmission. Also relevant to the present proceedings are rules 68C and 68D of the Prison Rules. They deal, respectively, with disclosure of intercepted material and with retention of intercepted material

[6] For present purposes, the Prison Rules in Northern Ireland are in very similar terms to the equivalent rules in England & Wales, the Prison Rules 1999 (SI 1999/728). In particular, rules 68A to 68D are materially similar to rules 35A to 35D of the analogue English rules. In both cases, section 49 of Investigatory Powers Act 2016 is relevant. It provides that conduct involving interception taking place in a prison is authorised by that section if it is conduct in the exercise of any power conferred by or under the relevant prison rules in England & Wales, Scotland, or Northern Ireland.

Factual background

[7] The factual background to this case may be briefly stated. At the material time the applicant was a prisoner in HMP Maghaberry, held on remand in relation to alleged driving offences. He has mental health problems, including paranoia. Details of these issues are set out in his grounding affidavit but need not be repeated for present purposes. It suffices to say that the applicant has averred that his paranoia has become a dominant aspect of his mental health, particularly when he is in custody. He seeks an understanding of the prison authorities' approach to the monitoring of communications in order to 'stabilise his mental health' and so as to be better able to understand the limits placed upon telephone surveillance. In particular, he contended that it was difficult for him to talk on the telephone with a variety of friends and relatives and he has found it difficult to write freely to his mother. The resulting inhibition has, he considers, further negatively impacted his mental health. Those issues were plainly enough to give him standing to bring the proceedings (the issue of victim status for the purpose of relying on Convention rights is dealt with separately below); but this case is not dependent upon the applicant's mental health issues: his argument is that the legal protections applicable to all prisoners have not been respected.

[8] The respondent's position is set out in an affidavit from Mr Alcock, the Deputy Director of Security and Operations of NIPS who, inter alia, has operational oversight of the use of investigatory powers by the Prison Service. Guidance for operational staff working in this area is provided in the NIPS Security Manual, some relevant extracts from which were exhibited to Mr Alcock's affidavit. It is generally

"restricted to internal use only for reasons of operational security." In addition, reference is made to Standing Order 5 of the NIPS Standing Orders, which is publicly available but largely deals with interception of letters and written communications.

[9] It is common case that a 'compact' is provided to prisoners dealing with these issues and that the applicant was in receipt of this document. Prisoners are asked to read this and sign it, after which (the applicant avers) it is removed from them. Instead of their being given a copy, it is placed in a file. The respondent's evidence is that the compact is explained to prisoners; and that it is retained on their 'wing file.' I return to the content of the compact in a moment. The version which the applicant signed after being received into prison was in evidence before me.

[10] The respondent's evidence explains that there is routine and automatic recording of all telephone calls, except for a limited category of legal and privileged communications from and to prisoners (referred to below for convenience as "confidential calls"). However, although calls are recorded, these are not accessed except where this is considered necessary, justified, and proportionate. I interpose that the mere recording of a call constitutes interception of it for the purposes of rule 68A: see rule 68A(6)(a). In these proceedings and in its documentation, the respondent has tended not to use that word. Rather, it refers to 'recording' and then 'monitoring.' 'Monitoring' is used to refer to prison staff actually listening to the content of a telephone call, which will sometimes (although rarely) occur simultaneously to the call being made and will more often occur, where authorised, by a recorded call being played back. For ease of understanding, I have used the terms in this way throughout this judgment.

[11] Mr Alcock's affidavit also contains an averment that none of the applicant's calls had been monitored to date (that is to say, albeit they had been recorded in common with other calls, the recordings had not been accessed and listened to). Specific monitoring is authorised on a regulated and case-by-case basis, with a separate application process required, which has Security Governor oversight. Mr Alcock exhibited a copy of the appropriate pro forma – the Monitoring of Communications Intelligence Led Authorisation Form – as the means of explaining the process of authorising such monitoring. In addition, he explained that, in rare emergency situations, it may be necessary to carry out authorisation for the interception of communications immediately (for instance, where there was a potential threat to life or safety). In those circumstances, an Immediate Response Monitoring (IRM) process is followed. Again, Mr Alcock averred that the applicant had not been subject to the interception of his communications by either of these means.

[12] When prisoners are received into prison, a Communications Compact Induction document is provided to them which explains telephone use within the prison in simple terms. It advises prisoners that, "Your phone calls to friends and family are recorded and may be monitored." It also advises that if the prisoner is

calling their solicitor or MP, they should let the prison know and these calls will not be monitored.

[13] The compact itself is in more detailed terms. It contains a note to staff indicating that it must be explained to all prisoners; and that prisoners must sign a copy of the compact before being allowed to use the PIN phone systems. The signed copy is then stored on the prisoner's wing file. I understand from Mr McGleenan's submissions that this can then be consulted again by the prisoner upon request. I certainly see no reason why it should not be able to be so consulted if a copy is not left with the prisoner for reference. There are a variety of terms and conditions of use of the PIN phone system contained within the compact. These include the following:

> "4. **CONVERSATIONS WHICH TAKE PLACE USING PRISON PIN PHONES WILL BE RECORDED AND MAY BE MONITORED BY PRISON STAFF. PIN PHONES CAN BE USED ONLY BY PRISONERS WHO CONSENT TO THIS.**
>
> 5. The exception to paragraph 4 is that calls to your legal advisers (as notified by you to the PIN phone clerk), courts, or Confidential Access organisations are confidential and will not be recorded or monitored except where there is reasonable cause to believe that the calls are intended to further a criminal purpose. The decision to monitor these calls will be taken only on the authority of the Director General of the Northern Ireland Prison Service (NIPS) or the Director of Operations of NIPS. In such circumstances recording will continue for no longer than necessary to establish the facts and to take any action necessary."
>
> [bold emphasis in original]

[14] Further information on monitoring is contained in the following portion:

> "Prisoners may be subject to specific monitoring for the following reasons:
>
> - Prisoners who are identified as posing a risk to children;
> - Prisoners remanded for, or convicted of, an offence of harassment, or subject to a restraining order or injunction. This must continue while an order/injunction is in force, and subsequently if deemed necessary;
> - Prisoners convicted of a serious sexual crime;

- Category A prisoners; where information suggests a prisoner may intimidate victims/witnesses."

[15] (It seems likely that the reference to situations where information suggests that a prisoner may intimidate victims or witnesses should be contained in a separate bullet point and is not restricted to monitoring Category A prisoners where such a situation exists, as might be suggested by the use of the semi-colon in the last bullet point.)

[16] In addition, prisoners are advised at para 8 of the compact that, "A maximum of up to 5% of all other calls made on the PIN phones system are subject to monitoring on a daily basis." The applicant's evidence suggests that he was principally concerned about this residual category of monitoring.

[17] The compact also provides information about communication by way of letters and includes the following:

> "A maximum of up to 5% of the correspondence sent and received on a daily basis by prisoners is subject to monitoring. All mail, except legally privileged or to a confidential access organisation… may be opened to check for illicit enclosures and may be subject to monitoring."

[18] Again, examples are given of letters which may be read, and a range of risk factors are mentioned (which overlap heavily with those quoted at para [14] above). In the case of both telephone calls and written communications, prisoners are warned about various types of behaviour which are unacceptable and may result in disciplinary action. I need not set these out but many of them are predictable, e.g. planning criminal activity or offences against prison discipline or seeking to communicate in coded messages.

The applicant's complaints

[19] The applicant contends that the published compact is inconsistent with the 'unpublished material' (namely, internal documents which have been exhibited to Mr Alcock's affidavit for the purpose of these proceedings). For example, one of the applicant's main complaints is that he suffers from paranoia and that this prevents him from speaking freely on the telephone. In light of this, he contends that "in order to assist him with rationalising his fears and understanding the extent to which he can be monitored", he should be able to clearly see the circumstances in which his calls can be intercepted and the potential frequency of such an occurrence. In this regard, the applicant complains that, in light of what is set out in the compact and quoted at para [16] above, any officer can listen to his private and intimate calls each day, provided those calls are within the 5% of calls monitored. It is not indicated in the compact whether this element of call monitoring is random, or whether an officer may arbitrarily target the calls of a particular prisoner (provided their calls do not

exceed the 5% threshold). He also points to an absence of clarity or precision as to which officers have the authority to listen to calls, or what is done with any recordings in terms of storage or dissemination. In addition, he observes that little if any explanation is provided as to what the 5% figure means in real terms (for instance, whether it relates to 5% of the number of calls made or 5% of the total call time).

[20] In submissions, Mr Hutton also suggested that the prison authorities should explain how they approached which "class" of prisoner was the subject of directions under rule 68A(1) and how the grounds upon which such directions might be given in rule 68A(4) (which differ from those set out in rule 67(3)) are approached and applied. He further argued that there must be some process in respect of such monitoring – since NIPS had suggested in its pre-action response that monitoring was subject to strict control and oversight – but that no further explanation of this process had been provided to prisoners.

[21] In its response to pre-action correspondence, NIPS explained again that there was routine recording of all telephone calls to and from prisoners, except for legal and privileged communications (for example with legal representatives or Members of Parliament). Those calls which are recorded, however, "are not routinely accessed, save on a random sample basis or where deemed necessary, and are deleted from the remote system location automatically after a set period of time, in compliance with data protection requirements." In addition, it was explained, in similar terms to those later contained in Mr Alcock's affidavit evidence, that specific monitoring is authorised on a case-by-case basis, where this was deemed necessary, justifiable, and proportionate; and that this was subject to a separate application process with Security Governor oversight. No more detail about this process was provided at that point. NIPS also contended that the applicant, and indeed all prisoners, are informed in their communications compact that all calls are recorded and may be monitored; and that there are also signs to this effect located prominently around the telephone area in the prison. On this basis, the respondent contends that its approach is sufficiently clear.

[22] In the portion of the Security Manual which has been exhibited, the concept of random monitoring is described in the following way:

> "Random listening
>
> 27.48 Telephone calls by prisoners not subject to routine listening, other than calls to their legal advisers or the Samaritans, may be selected for listening on a random basis, provided the Governor is satisfied that this is necessary and proportionate to the interests set out in Rule 67.

27.49 The percentage of random listening will be agreed with the Director of Operations and recorded in the Establishment's Contract."

[23] As to this, the applicant complains that it fails to define what is meant by "random" and how such random listening is to be conducted; but argues that, if this section of the Security Manual had been published, it would at the very least have informed prisoners that there was random listening.

[24] The applicant further contends that other matters contained in the Security Manual (not all of which was disclosed in the course of these proceedings) should be disclosed to prisoners, including the sections on reviews, record keeping, security around the intelligence that is gathered, how and in what circumstances live stream monitoring will take place and how long it can last, and what rank of officer is required to permit certain types of monitoring.

[25] In support of his case, the applicant has referred to Prison Service Instructions (PSIs) from England & Wales – PSI 49/2011 entitled 'Prisoner Communication Services' and, more particularly, PSI 04/2016 entitled 'Interception of Communications in Prisons and Security Measures' – which, he contends, provide a much better model of transparent explanation to prisoners of how interception of communications will be conducted. PSI 04/2016 ("the Interception PSI") describes a system which seems to closely mirror the arrangements in HMP Maghaberry as they have been disclosed in these proceedings, namely that for most prisoners all telephone calls (save for a limited category of confidential calls) are recorded but only a small number are actively monitored contemporaneously or by means of being listened back to. It also discloses that the primary means by which prisoners are to be shown to have understood this is, as here, by means of a communications compact. (I understand the Interception PSI has very recently been cancelled and replaced by another document published by HM Prison and Probation Service in England, entitled 'Authorised Communications Controls and Interception Policy Framework'; but that document was not in force at the time of argument in the present case.)

[26] The Interception PSI gives some further information as to what would here be termed 'targeted monitoring,' It explains that an initial risk assessment will be undertaken. The Interception PSI "and the Official-Sensitive version" are said to provide "the means to achieve a dynamic, intelligence-led approach to prisoner interception" (see para 2.13). I take it from the reference to a sensitive version, with an additional protective marking, that there is a further version of the PSI which is *not* available to the public or prisoners. "E-List Prisoners", who represent a heightened risk category, will have all calls (except legal and confidential calls) simultaneously monitored, with this categorisation being reconsidered monthly. Such prisoners must pre-book their telephone calls. In addition, the PSI describes processes for 'immediate response monitoring' and 'intelligence led monitoring', which are further situations in which monitoring may be undertaken for reasons

specified in the relevant Prison Rules. Finally, it deals with random monitoring, which is said to be "afforded the lowest priority within the interception arrangements in a prison," Random monitoring is said to allow prisons to uncover new risks or threats or prisoners of interest. It must usually be no more than 5% of mail and telephone calls each day; and all such monitoring undertaken must be recorded on the random monitoring log. Terrorism prisoners are subject to 100% monitoring of mail and telephone calls. Additional procedures relevant to Category A prisoners are also set out in the PSI.

[27] The monitoring forms provided in the respondent's evidence suggest that in Northern Ireland there is also a process by which specific monitoring of a prisoner (on the basis of intelligence) is requested. An authorisation is sought by the Security Team, who must set out the reasons as to why they consider the monitoring necessary. This is then considered by a governor or "competent manager as delegated by the Governing Governor of the establishment," They must consider the request and adjudicate upon it, identifying the reason why monitoring is considered necessary (if that be the case) and setting the parameters of the monitoring permitted (e.g. either in real time or by accessing recordings) and the timescale for this, including when the authorisation should be reviewed. A similar application process exists for authorisation for IRM monitoring, with more limited reasons potentially justifying this step and in circumstances where such monitoring "must usually be undertaken for a period of no more than five days from the date of an original intelligence report or the date of the incident and where appropriate five days going forward." Again, reasons must be provided for such a request and the authorising manager (the Security Governor or, in the case of absence or urgency, another Governor) must consider it to be proportionate. The potential urgency of such situations allows for verbal authorisation with written authorisation then granted retrospectively. The detail of these processes have been gleaned from the pro formas provided by Mr Alcock in his evidence. Unlike in the Interception PSI in England & Wales, this detail is not publicly available, nor generally available to prisoners. They are told merely that their calls "may be monitored."

Summary of the parties' positions

[28] The applicant argues that there is a requirement upon NIPS to publish its policy in relation to these matters, which arises both under common law and by virtue of article 8 ECHR. As the case developed, it became clear that the applicant was really arguing for disclosure of relevant portions of the Security Manual and, if separate, any internal procedures governing the obtaining of authorisation for targeted monitoring. He submits that this is a policy which regulates extremely invasive powers, including the power to listen in to conversations of the utmost sensitivity. Prisoners are entitled to regulate their conduct in a way that will lessen the opportunity for their otherwise private and sometimes intimate conversations to be intercepted, which cannot happen unless they see the full circumstances under which interception is regulated and applied.

[29] He further argues that matters such as these are important for all prisoners but, in particular, for paranoid prisoners such as him who damage their mental well-being by obsessing over matters such as malicious intelligence from other prisoners resulting in their calls being permanently monitored. Only through the publication of the policy can this be mitigated as it creates legal certainty for all involved.

[30] In submissions, Mr Hutton KC also suggested that the prison authorities should explain how they approached which "class" of prisoner was the subject of directions under rule 68A(1) and how the grounds upon which such directions might be given in rule 68A(4) (which differ from those set out in rule 67(3)) are approached and applied. He further argued that there must be some process in respect of such monitoring – since NIPS had suggested in its pre-action response that monitoring was subject to strict control and oversight – but that no proper explanation of this process had been provided. He pointed to a number of outdated references or errors, particularly in the portion of the Security Manual which was disclosed, and suggested that one purpose behind the obligation to publish was in order that such issues could be identified and corrected.

[31] The respondent contends that the applicant does not have the requisite victim status required by section 7 of the Human Rights Act 1998 (HRA) in order to rely upon his article 8 rights, since it has been confirmed on affidavit that he has not been the subject of any monitoring during the course of his detention. It contends that there is no common law obligation to publish a policy in this field and that, insofar as article 8 ECHR is concerned, it has met its 'quality of law' obligations by prisoners having access to the Prison Rules and the individual compact dealing with these matters. There is no obligation, Mr McGleenan KC submitted, to provide prisoners with any greater information in respect of the respondent's use of its powers under rule 68A than that which the applicant already had.

Failure to publish the policy at common law

[32] The applicant cited Auburn, Moffett and Sharland, *Judicial Review: Principles and Procedures* ("Auburn"), at section 21.64, which includes the following:

> "Legislation may require that a policy or guidance be published. However, where there is no such requirement (e.g. where a policy or guidance is non-statutory), the question arises of whether there is a duty to publish the policy or guidance (or, at the least, to make it available to the individuals who may be affected by the exercise of the relevant discretion). There has been a clear trend of the courts requiring the publication of policies, and that approach has been confirmed by the Supreme Court in *R (Lumba) v Secretary of State for the Home Department*."

[33] It is then further noted at section 21.69, as follows:

> "In cases where an interference with a Convention right can only be justified if the interference is 'in accordance with the law' or 'prescribed by law', the law must be sufficiently accessible to the individual. Accordingly, where a policy or guidance as to how an administrative discretion will be exercised constitutes part of the 'law' for that purpose, the policy or guidance will be subject to the same requirement of accessibility. It is difficult to see how this requirement could be satisfied unless the relevant policy or guidance is published."

[34] The applicant placed significant reliance upon the case mentioned by the authors, *R (Lumba) v Secretary of State for the Home Department* [2012] 1 AC 245. In that case, the Secretary of State had two policies in relation to the exercise of a discretion regarding immigration detention, one published and the other unpublished. At para [34] of his judgment, Lord Dyson said this:

> "The rule of law calls for a transparent statement by the executive of the circumstances in which the broad statutory criteria will be exercised. Just as arrest and surveillance powers need to be transparently identified through codes of practice and immigration powers need to be transparently identified through the immigration rules, so too the immigration detention powers need to be transparently identified through formulated policy statements."

[35] At para [302], Lord Phillips added the following:

> "I agree with Lord Dyson that, under principles of public law, it was necessary for the Secretary of State to have policies in relation to the exercise of her powers of detention of immigrants and that those policies had to be published. This necessity springs from the standards of administration that public law requires and by the requirement of art 5 that detention should be lawful and not arbitrary. Decisions as to the detention of immigrants had to be taken by a very large number of officials in relation to tens of thousands of immigrants. Unless there were uniformly applied practices, decisions would be inconsistent and arbitrary. Established principles of public law also required that the Secretary of State's policies should be published. Immigrants needed to be able to ascertain her policies in order to know whether or

> not the decisions that affected them were open to challenge."

[36] A range of other authorities were also relied upon by the applicant to similar effect. For instance:

(a) In *R (Walmsley) v Lane* [2005] EWCA Civ 1540, Sedley LJ noted at para [57] that:

> "It is no part of this court's task to say what such a policy should contain. But it is right to say that it is inimical to good public administration for a public authority to have and operate such a policy without making it public…"

(b) In *B v Secretary of State for Work and Pensions* [2005] EWCA Civ 929, Sedley LJ was again dealing with the failure to publish a policy, when he said the following (at para [43]):

> "If… a policy has been formulated and is regularly used by officials, it is the anthesis of good government to keep it in a Departmental drawer."

(c) In *R (McMorn) v Natural England* [2015] EWHC 3297 (Admin), the English High Court was dealing, inter alia, with a failure to publish a policy on how licence applications were dealt with in respect of killing certain birds. In granting the application on the failure to publish ground, Ouseley J said the following (at para [150]):

> "… if a public body has a policy to guide its decisions, lawful decision-making requires that the policy should be public, and the more so that the policy should not be concealed behind a partially different policy."

(d) The applicant further relies upon *R (Salih) v SSHD* [2003] EWHC 2273 (Admin), in which it was said at para [52] to be a "constitutional imperative" not to withhold information about a policy relating to the exercise of a statutory power, in that the statute is published and so should the guidance on how it is applied.

(e) To like effect, it had been said in *R v Chief Constable of the North Wales Police, ex p AB* [1999] QB 396, at 429H, that:

> "… both so as to accord with the principles of good administrative practice and to comply with the

> requirement that a public authority should act 'in accordance with the law'… [the police] should have made the policy which it was applying available to the public. To do so provides a safeguard against arbitrary action."

[37] The applicant also considered it highly significant that NIPS has previously relied upon a combination of the 1995 Rules and unpublished associated policy guidance in order to appeal the decision in *Re Flannigan's Application* [2016] NIQB 27, a case involving the recording of strip searches. There is no reported judgment in that case; but the applicant contends that the Lord Chief Justice indicated a view on behalf of the Court of Appeal to the effect that the failure to publish the associated policy was fatal to the appeal. I am afraid I am able to give little weight to this (anecdotal) argument in the absence of any written judgment and the different context of the present challenge.

[38] In any event, for those reasons the applicant submits that the common law requires a transparent statement outlining the circumstances in which broad statutory criteria will be exercised; and that therefore the failure by the proposed respondent to promulgate a policy (or publish its full policy) in respect of the interception of communications and related security matters was therefore unlawful. Put another way, he also submits that, in light of the fact that there was no bar to NIPS disclosing aspects of the policy for the purpose of these proceedings, it had been demonstrated that no good reason existed to have kept it "secret" in the first place.

[39] The respondent contends that, in a range of cases of the highest authority, it has been confirmed that the common law does not require a transparent statement outlining the circumstances in which broad statutory criteria will be exercised. On the contrary, the respondent argues, the common law has recognised that there is no absolute duty in this regard. Mr McGleenan also relied upon the judgment of the Supreme Court in *Lumba* at para [38]; and on the decision of the Court of Appeal in this jurisdiction in *Re McCord's Application* [2020] NICA 23; [2021] NI 318, to which I return below. At para [38] of his opinion in *Lumba*, Lord Dyson said this:

> "The precise extent of how much detail of a policy is required to be disclosed was the subject of some debate before us. It is not practicable to attempt an exhaustive definition. It is common ground that there is no obligation to publish drafts when a policy is evolving and that there might be compelling reasons not to publish some policies, for example, where national security issues are in play. Nor is it necessary to publish details which are irrelevant to the substance of decisions made pursuant to the policy. What must, however, be published is that which a person who is affected by the operation of the policy needs to

> know in order to make informed and meaningful representations to the decision-maker before a decision is made."

[40] There was some debate about whether national security was in play in the present case – but that was simply an example given of one area where there may be compelling reasons for a policy (or all of the relevant detail of a policy) not to be disclosed. That a different approach might be warranted or required at common law in cases involving national security, or other like contexts, is referenced in a number of the authorities (see also, for instance, para [52] of the *Salih* case referred to above).

[41] Important points arising from the *Lumba* decision about the publication of policies applied by public authorities are that an unpublished policy should not be inconsistent with a published policy, so to mislead (see para [20] of *Lumba*); and that a policy which is applied should be published if it will inform discretionary decisions in respect of which the potential object of those decisions has a right to make representations (see paras [20], [35] and [38] of *Lumba*). These are essentially requirements of procedural fairness.

[42] The Court of Appeal decision in *McCord* contains some helpful commentary on the question of publication of policies but, broadly, I accept the applicant's submission that it is of limited assistance because of the context in which it arose. That case was, to a large degree, about a putative obligation to *formulate* a policy (to govern when a border poll ought to be called) where one was not in place. It was not a case about non-disclosure of a formulated policy. Nonetheless, it is relevant to note that at para [33] the Court of Appeal cited, with no caveat or disapproval, a number of principles underpinning the judge's reasoning below. These included that "there is no generally applicable common law requirement for public bodies to publish guidelines establishing how statutory powers will be exercised, the factors which will be taken into account or the sources of evidence." On the facts of that case, it had been rational for the respondent not to publish a policy, since an attempt to pre-determine the factors to be taken into account or the evidence to be relied upon may have proven unduly restrictive and not in the public interest. Moreover, a policy worded in undefined and flexible terms would add nothing to the existing statutory wording and it was rational for the respondent not to adopt such a policy.

[43] Ultimately, I accept the respondent's submission that the common law has recognised that the requirements relating to the formulation and publication of policies as to how statutory powers will be exercised are context specific. A further example of this is *Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others* [2019] UKIPTrib IPT 17/186/CH: see paras [86]-[89]. Referring back to *Lumba*, the Investigatory Powers Tribunal (in the lead judgment given by Singh LJ, Lord Boyd, and Sir Richard McLaughlin) quoted Lord Dyson in para [38] of *Lumba*, pointing out that what must be published "is that which a person who is affected by the operation of the policy needs to know in order to make informed and meaningful representations to the decision-make before a decision is

made." In the context the Tribunal was dealing with, involving the activities of the intelligence services, the Tribunal went on to say: "That principle, which lies beneath the requirement of publication of a policy in the context of a case such as *Lumba*, obviously has no application to the present context." As I have suggested above, at common law it is often helpful to consider this issue as a sub-category of the obligation to act in a procedurally fair manner.

[44] In the present case, I do not consider that there is a common law obligation requiring the applicant to be given greater information about when his calls may be listened to or his letters monitored. This is not a context where the applicant has a role to play by, for instance, opposing an application for an authorisation that his calls be monitored. Rather than a broad statutory discretion which directly affects his interests, this case concerns an investigative power, exercisable only on certain grounds spelt out in the Prison Rules, by the prison authorities.

[45] In contrast, many if not all of the cases upon which the applicant relies in order to seek to establish that there is a requirement at common law to publish a policy arise in the context of administrative adjudications. In some cases they merely contain obiterstatements which might be regarded as indicating good practice rather than a binding legal requirement (for instance, the *ex parte AB* case). I accept the respondent's submission that the statutory power under the Prison Rules which is at issue in this case is of a different nature and cannot be equated to adjudicative functions such as those that were under consideration in cases such as *R (Walmsley) v Lane* (the discretionary power not to enforce a congestion penalty charge); the *B* case (the discretion not to seek recovery of overpaid benefits); *McMorn* (an environmental application for a licence to kill certain wild birds); *Salih* (non-publication of policy defining eligibility for asylum support); or *ex parte AB* (regarding a police decision to disclose details of previous sexual offending against children).

[46] The respondent also relies upon the decision in *R (BF (Eritrea)) v Secretary of State for the Home Department* [2021] UKSC 38 in support of the contention that no common law obligation exists for a public authority to issue policy guidance in an attempt to eliminate uncertainty in relation to the application of a particular legal rule. Lord Reed stated at para [52] that:

> "Save in specific contexts oof a kind discussed below and in our judgment in the *A* case, there is no obligation for a Minister or anyone else to issue policy guidance in an attempt to eliminate uncertainty in relation to the application of a stipulated legal rule. Any such obligation would be extremely far-reaching and difficult (if not impossible in many cases) to comply with. It would also conflict with fundamental features of the separation of powers. It would require Ministers to take action to amplify and to some degree restate rules laid down in legislation, whereas it is for Parliament to choose the rules

> which it wishes to have applied. And it would inevitably involve the courts in assessing whether Ministers had done so sufficiently, thereby requiring courts to intervene to an unprecedented degree in the area of legislative choice and to an unprecedented degree in the area of executive decision-making in terms of control of the administrative apparatus through the promulgation of policy."

[47] When properly analysed the power at issue in this case (to conduct surveillance in the context of prison communications) does not in my view require and is not amenable to the publication of a policy in the nature contended for by the applicant, explaining in great detail when communications will be monitored. If a prisoner was able to predict with certainty when a communication would be intercepted the purpose for which the power has been conferred may be wholly undermined.

[48] In these circumstances, the statutory scheme and the information provided to the applicant (particularly as contained in the compact), taken together, are in my view sufficient to allow the applicant to both understand NIPS's powers and the circumstances in which they will or may be exercised. The level of disclosure contended for by the applicant at some points (including setting out the detail of how each basis for interception would be addressed) could give rise to concerns about the operational effectiveness of the exercise of the powers on behalf of NIPS and undermine the statutory purpose for which they were conferred. I do not consider there to be an obligation at common law to provide additional information. The applicant is aware of the origin of the interception power and the grounds upon which it can be exercised from the provisions of the Prison Rules. He is also aware from the compact that all calls are recorded (save for legal or designated confidential calls) and may be subject to specific monitoring where a risk-based reason for this exists.

[49] It is true that the compact does not specifically say that the residual daily monitoring of up to 5% of calls is to be conducted on a random basis; and that the Security Manual makes clear that this residual monitoring is to be random in nature (rather than arbitrarily targeted at an individual). At the same time, the Security Manual does not set the percentage of calls which can be monitored in this way. That is set out in the compact. However, reading the compact fairly and in the round, it seems to me that the most natural interpretation of it is that the residual monitoring will be conducted on a random basis, since this element of monitoring is described after all of the detail has been given about pre-approval of telephone numbers and matters which might result in *targeted* or specific monitoring. The reference to monitoring up to 5% "of *all other calls* made on the PIN phone system" is entirely consistent with that being conducted on a random, sampling basis. I do not accept that there is inconsistency in this regard between the unpublished material in the Security Manual and the contents of the compact.

[50] In summary, I do not consider there was an obligation at common law for the applicant to be told more than he was, over and above what was contained in the Prison Rules and the communications compact, about when monitoring of his calls would take place. These documents provided a sufficiently clear picture of the powers in play and how they would be used; and, in any event, it was not necessary for the applicant to know more for the purposes of making representations to the prison authorities, since (whether dealing with targeted monitoring on the basis of intelligence or selection of his communications by way of random sampling) this was not a process in which he enjoyed the right of participation.

Article 8 ECHR

[51] I turn then to the alternative basis upon which the applicant's case was mounted, namely article 8 ECHR. There is some overlap between the analysis at common law and that required by the Convention but the Convention requirements of legality, in my view, go further than the requirements of the common law. They are focused not on the question of fairness (although article 8 may have procedural aspects) but on the accessibility of the relevant provisions by which privacy rights may be lawfully interfered with and transparent demonstration of the safeguards which exist against arbitrary interference with qualified rights.

[52] First, I am not persuaded that the applicant lacks sufficient victim status to rely upon his article 8 rights in this case simply because he has not (yet) had any calls monitored. His case is that he should be provided, by means of publication of the relevant policy or guidance documents, with further information as to when he is *liable* or likely to have his calls listened to and how any such decisions will be made. The mere fact that he is detained in prison and is at risk of this in light of the approach adopted by NIPS is, in my view, sufficient to provide him with the necessary status under section 7 HRA.

[53] A person wishing to rely on Convention rights under section 7 must show that they are *or would be* a victim of the unlawful act. In some circumstances, being a potential victim is sufficient. That is clear, for instance, from the judgment of Morgan LCJ in *Re JR1's Application* [2011] NIQB 5, at paras [38]-[41]. The judge there cited and applied an earlier decision of the Court of Appeal, *Re NI Commissioner for Children and Young People's Application* [2009] NICA 10. Victim status can be established where the claimant, although not yet affected, can show the potential for his or her own rights to be affected. Whether the connection or risk of being affected is sufficient is a matter of fact and degree. (In *JR1's Application*, Morgan LCJ was not persuaded that the applicant was sufficiently at material risk in order to warrant victim status. I reached a different conclusion, in a different context, in *Re JR159's Application* [2021] NIQB 68: see para [73].) In the present context, a relatively liberal approach to victim status has been taken, so that applicants must demonstrate that, as a result of their personal circumstances, they are potentially at risk of having their communications intercepted (see Harris, O'Boyle and Warbrick, *Law of the European*

Convention on Human Rights (5th edition, 2023, Oxford), at p 538, commenting on the Grand Chamber decision in *Roman Zakharov v Russia* (App No 47143/06)).

[54] In this case, it is clear that all calls are recorded, albeit that only a much more limited category of recorded calls are accessed. The applicant will therefore have had his telephone calls recorded and they are available for monitoring. He might also be subject to residual random monitoring. Whilst a prisoner, he is clearly at risk of being affected by NIPS's actions which he contends are unlawful. On a similar basis, I reject the proposed respondent's argument that the case is entirely academic merely because the applicant had not (at the time of the evidence being filed in these proceedings) had any of his calls intercepted.

[55] Article 8 does not directly require publication of any particular policy on the part of a public authority. However, where interference with a qualified right is concerned, it does require this interference to be "in accordance with law." One aspect of the requirement is an element of foreseeability and transparency. In the *McCord* case referred to above, it was recognised that "where the exercise of statutory powers may interfere with Convention Rights and where the interference must be 'in accordance with law', the quality of law test may require guidance in order to avoid arbitrariness and to ensure that the law is sufficiently accessible and predictable." The extent to which this will be required is, however, again dependent upon the particular context.

[56] In submissions, Mr Hutton properly conceded that there is a balance to be struck and that Article 8 "does not need every jot and tittle to be disclosed." Nonetheless, the applicant relied upon the case of *Malone v United Kingdom* (App No 8691/79) – a case which arose in the context of surveillance – in which the ECtHR said this at para 67:

> "The Court would reiterate its opinion that the phrase "in accordance with the law" does not merely refer back to domestic law but also relates to the quality of the law, requiring it to be compatible with the rule of law, which is expressly mentioned in the preamble to the Convention… The phrase thus implies… that there must be a measure of legal protection in domestic law against arbitrary interferences by public authorities with the rights safeguarded by paragraph 1 (art. 8-1)… Especially where a power of the executive is exercised in secret, the risks of arbitrariness are evident… Undoubtedly, as the Government rightly suggested, the requirements of the Convention, notably in regard to foreseeability, cannot be exactly the same in the special context of interception of communications for the purposes of police investigations as they are where the object of the relevant law is to place restrictions on the conduct of individuals. In particular,

> the requirement of foreseeability cannot mean that an individual should be enabled to foresee when the authorities are likely to intercept his communications so that he can adapt his conduct accordingly. Nevertheless, the law must be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to this secret and potentially dangerous interference with the right to respect for private life and correspondence."

[57] It is important to note that there are obligations to ensure an adequate indication of both the *circumstances in which* and the *conditions on which* interference may lawfully occur. In my view, it is helpful to consider these separately. The Court went on to note that, in complying with the Convention, these two issues may be addressed in administrative materials: the detailed procedures and conditions to be observed do not necessarily have to be incorporated in rules of substantive law. Continuing, at para 68, the ECtHR went on to say this:

> "The degree of precision required of the "law" in this connection will depend upon the particular subject-matter (see the above-mentioned *Sunday Times* judgment…, para. 49). Since the implementation in practice of measures of secret surveillance of communications is not open to scrutiny by the individuals concerned or the public at large, it would be contrary to the rule of law for the legal discretion granted to the executive to be expressed in terms of an unfettered power. Consequently, the law must indicate the scope of any such discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity, having regard to the legitimate aim of the measure in question, to give the individual adequate protection against arbitrary interference."

[58] A restatement of relevant principles is also contained in the Grand Chamber's judgment in the *Zakharov* case mentioned above, at paras 227-234. This, again, recognises that foreseeability in the special context of interception of communications cannot mean that an individual should be able to foresee when the authorities are likely to intercept his communications so that he can adapt his conduct accordingly. However, given the risks of arbitrariness, "it is therefore essential to have clear, detailed rules on interception of telephone conversations…" The court has developed "minimum safeguards that should be set out in law in order to avoid abuses of power", which include "the procedure to be followed for examining, using and storing the data obtained." That is necessary in part because, in in assessing whether there are adequate and effective guarantees against abuse so that

interferences are Convention compliant, the assessment depends on all the circumstances of the case. That will include the procedures for supervising the ordering and implementation of the restrictive measures.

[59] I have not been persuaded that the applicant requires more information on the circumstances in which his calls may be monitored. He is aware that all calls are recorded. He is also aware, or ought reasonably to have been aware, that specific monitoring only occurs where some risk-based factor is considered to justify it, with those factors being those specified in rule 68A(4)(a)-(e); and that limited residual monitoring occurs on a random basis. As the *Malone* judgment recognises, in this context, there are limits to the requirements of foreseeability. I consider that there is "an *adequate* indication as to the circumstances in which" the applicant's calls will be accessed, set out in the Prison Rules themselves and the communications compact which was provided to him.

[60] There is nonetheless the separate question of whether prisoners are given an adequate indication of the *conditions on which* interference (in this case, monitoring) may lawfully occur; or, put another way, whether prisoners are provided with an adequate indication of the manner of the exercise of the discretion. NIPS has quite properly built in a range of safeguards to ensure that the more intrusive element of accessing call content can only occur where appropriate authorisation is given (or, in the case of random listening, only to a limited extent). However, little or no details about this are made available to the public or to prisoners. As noted above, they are simply told that their recorded calls "may" be monitored, with some indicative reasons for such monitoring then specified.

[61] There is no published direction to a governor from the Department under rule 68A(1). (It is unclear whether the Security Manual is considered to amount to such a direction but that is unlikely since it is described by Mr Alcock as "guidance for operational staff.") It seems, rather, that the interception regimes is set out in "arrangements" which have been made pursuant to rule 68A(2) to the effect described above. Those arrangements include the routine recording of all non-confidential calls. Although not expressly explained to prisoners, in my view the reason for this is self-evident, namely to allow access to recorded content where the necessity for this later becomes clear but where, in the absence of recording, the opportunity to do so would have been lost.

[62] Mr Hutton was right to observe that prisoners are given very little or no detail as to how the process of authorisation of specific monitoring is to be conducted. It is this process which provides the important safeguards and oversight to which the respondent has referred (and which would no doubt be relied upon by NIPS in the event that a more substantive challenge was mounted to the legality or proportionality of the arrangements it has put in place). However, prisoners are merely told in the compact that their calls "may be subject to specific monitoring" for certain reasons (which are inexhaustive). They are told nothing of the procedure relating to this.

[63] The conditions which require to be met before specific monitoring can occur are now reasonably clear to me from the internal forms which have been exhibited by the respondent (see para [27] above). One might well guess that the basis for specific monitoring would be tied to the statutory test set out in rule 68A(4) and (5). That appears to be correct but is not explained to prisoners. More importantly, nowhere are prisoners advised of how authorisation is sought or provided; and who is in a position to grant it. Looking at rule 68A(2), it is the governor who makes the primary determination on what is necessary in terms of interception of communications. An officer or authorised employee may terminate a call during transmission under rule 68A(3) but, otherwise, is not provided with any express decision-making responsibility under the rule. It seems to me that it would be quite permissible for the governor to make arrangements providing officers or authorised employees (or other governors) with a decision-making role as part of the arrangements he or she considered necessary. But where this is done, it should be capable of being understood by those liable to be affected by the process.

[64] The procedures which are apparent from the internal forms which have been put in evidence find no expression or description in the respondent's Standing Orders, nor in the Prison Rules, nor indeed in the communications compact provided to prisoners. The disclosure of information about those procedures in the course of these proceedings and the relatively detailed description of similar or equivalent procedures in the course of the Interception PSI which applied in England & Wales has persuaded me that there is no proper reason why additional information about these processes could not, or should not, be provided to prisoners. Providing details of the authorisation process would not undermine the purpose of the interception power in the same way as seeking to define precisely when authorisation will be granted might do.

[65] I reject the broad submission that, merely because the proposed respondent has produced additional documentation to the court in these proceedings in the context of the discharge of its duty of candour, it follows that there was no proper basis for them not to have been disseminated to prisoners as a matter of routine. That is too wide-ranging. However, the fact that certain materials or information have been disclosed in this way (whilst others have not) is relevant to court's determination of whether the respondent has complied with its Convention obligations to act "in accordance with law."

[66] On balance, I have been persuaded that the information made available as to how the powers under rule 68A will be exercised is inadequate to meet the requirements of the Convention. There must be safeguards against arbitrary or over-zealous monitoring of call content. That is clear both from article 8 itself and the provisions of rule 68A which are designed to mirror its requirements. Where the respondent has determined to record all non-confidential calls on a precautionary basis but to build in a further layer of decision-making before call content can be accessed, treating that monitoring as the effective point of interception, those liable to

be affected are entitled to basic information about how that system operates, so as to give them reassurance that they will be protected from arbitrary interference. As in the *Malone* case discussed above (see para 79 of that judgment), even though detailed procedures may exist, prisoners were not made aware of these with any degree of reasonable certainty and, thus, they would be liable to change at the discretion of the respondent.

[67] It is no answer to this point to rely upon the fact that the applicant, and his fellow prisoners, are incarcerated. It is well known that prisoners retain all civil rights which are not taken away expressly or by necessary implication (see *Raymond v Honey* [1983] 1 AC 1; and rule 2(1)(j) of the Prison Rules). As I have also mentioned above, rule 68A is also obviously drafted with a view to ensuring that article 8 protections are built into the regime maintained in prisons for the interception of prisoner communications. It is also a general principle applying to all prisoners, and with regard to which the Prison Rules were made, that prisoners shall be given facilities to maintain links with their families and encouraged to do so (see rule 2(1)(i)), to say nothing of the additional provisions from which the applicant should benefit as an untried prisoner under rules 97(2) and rule 101.

[68] I also accept that some additional information should be provided pursuant to article 8 obligations as to how random monitoring occurs, so as again to provide reassurance that unjustified interference is not occurring. There was no challenge in substance to the legality of conducting some element of random monitoring and I therefore proceed on the basis that it is lawful. I also accept that some element of arbitrariness is implicit in the notion of random monitoring. However, in order to provide a safeguard against random monitoring being used to circumvent the authorisation process, at least some indication should be given as to how calls are to be randomly selected (that is, to indicate how it is guaranteed that this element of monitoring is actually random, rather than targeted in some way but without complying with the usual authorisation procedures).

[69] As highlighted in the affidavit filed on behalf of the respondent, the use of investigatory powers by NIPS is subject to review by the Investigatory Powers Commissioner's Office ("IPCO"). The IPCO was established pursuant to Chapter 8 of the Investigatory Powers Act 2016. The Commissioner's role is to exercise independent oversight of the use of investigatory powers to ensure that they are used in accordance with the applicable statutory framework and in the public interest. The IPCO therefore represents an additional statutory safeguard which operates to ensure that a subject's rights are not unlawfully infringed. The respondent has quite understandably made the point that, despite having been subject to annual reviews, the IPCO has made no recommendations in respect of NIPS and the information it makes available to prisoners in respect of the interception of communications. Similarly, the IPCO has made no recommendation in respect of the publication by NIPS of a policy concerning the interception of communications.

[70] However, IPCO's view is not determinative of the legal issue before the court. Moreover, it seems likely that the Commissioner's focus will have been on the propriety and rigour of the authorisation procedures applied by NIPS rather than the more limited question addressed in these proceedings as to whether NIPS was required to provide more information about those procedures to those affected. Indeed, the IPCO reports provided by the respondent indicate that at inspections they aim to ensure that the correct authorisations and risk assessments are *completed*. That is a different issue from the question the court has been considering, as to whether those likely to have their article 8 rights interfered with are adequately informed in relation to the procedures for this. The IPCO reports indicate that it aims to ensure that inmates are aware that their communications are liable to be intercepted and that their confidential communications will not ordinarily be monitored. That information is indeed provided but, for the reasons given above, I consider that the respondent's obligations under article 8 go further. The IPCO reports note that, in England & Wales, detailed guidance on how interception should be carried out is provided in a number of documents including PSIs; but do not go on to compare the level of information provided in Northern Ireland.

[71] I do not intend to address in detail the applicant's further complaint that insufficient detail was provided in relation to the issue of retention of intercepted communications or disclosure outside the prison authorities. These matters are dealt with expressly in rules 68C and 68D of the Prison Rules. In any event, it is clear that this was not the focus of the present challenge and little argument was addressed to these issues. Likewise, little argument was addressed to the issue of interception of written correspondence in the form of letters, although this was raised in the applicant's affidavit evidence. As to that, it seems to me that the same considerations apply as discussed above in relation to telephone calls. That is to say, prisoners are appropriately advised that all non-confidential and non-privileged correspondence may be checked for illicit enclosures and that letters can be read in certain cases; but that insufficient information is provided in relation to the process of authorising when letters will be read so as to comply with article 8 (which is similar to the authorisation process for monitoring telephone calls).

Alternative remedy

[72] The respondent relied upon the existence of an alternative remedy in these proceedings as a reason for the refusal of leave. Initially, it was contended that the Investigatory Powers Tribunal (IPT) constituted an effective alternative remedy. However, that body does not appear to have jurisdiction in accordance with section 65 of the Regulation of Investigatory Powers Act 2000 (RIPA). That is now accepted by the proposed respondent. It is unnecessary to set out a detailed analysis of the statutory provisions which gave rise to this conclusion; but, in essence, it is because the conduct of which the applicant complains did not take place "in challengeable circumstances", as required in this case by section 65(4) of RIPA, read with section 65(7) and (8).

[73] However, NIPS has also raised the possibility of making a complaint under rule 75 of the Prison Rules (with an eventual right to pursue the matter to the Prisoner Ombudsman). The applicant contends that such complaints and investigations are limited to the following under rule 75, namely:

> "(a) his treatment by any person employed in the Northern Ireland Prison Service, including provision for his welfare while in prison, and treatment includes an omission;
>
> (b) the facilities available to him at the prison; and
>
> (c) the cleanliness and adequacy of prison premises."

[74] The applicant says that the subject matter of this application is the failure by NIPS to publish a policy in respect of the interception of communications, which he contends is unlawful. He considers that it is "highly doubtful" that this complaint would be entertained by the Prison Service under sub-paragraph (a) cited above, which would then be the end of the matter, as the Ombudsman is similarly restricted in what she can investigate.

[75] It seems to me that the subject of these proceedings is *capable* of being the subject of a complaint under rule 75(a). The applicant may well be right that the Prison Service would be reluctant to view it that way if he sought to raise the issue in that fashion. There may also be a respectable argument that the issue raised by the applicant does not concern his "treatment" in the prison, particularly because of NIPS's confirmation that his calls have not in fact been intercepted. However, in any event, I consider there to be force in the applicant's submission that the issue raised is an issue of law (viz whether there is a legal requirement upon NIPS to publish a policy document or further information about its interception processes) which – even if it could theoretically be addressed by the complaint mechanism – is classically a matter for the determination of the court. Even assuming, therefore, that the complaints system could address this issue (which is far from clear), I would in any event exercise my discretion to allow the case to proceed by way of judicial review.

Conclusion

[76] In summary:

(a) I reject the respondent's case that the court should not consider the application by reason of alternative remedy or the case being academic.

(b) I reject the applicant's case at common law that the respondent was required to publish its policy (or, more accurately, currently

unpublished documents provided for internal guidance) in relation to its interception of prisoner communications.

(c) I accept the applicant's case that the requirement for any interference with his article 8 rights to be 'in accordance with law' is not satisfied by the present level of information made available to the public and prisoners in some limited respects, namely in terms of the information provided to prisoners about the procedure for authorising real-time or subsequent accessing of the content of their calls. I reject the respondent's case that the applicant lacks victim status such as to be precluded from relying on his article 8 rights.

[77] I grant the applicant leave to apply for judicial review on both grounds but dismiss the application on the common law ground. The application is allowed on the Convention ground, on the basis set out above.

[78] I will hear the parties on the issue of costs and on the terms of any final order.

Postscript

[79] Subject to any appeal on the part of the respondent, I would anticipate that one result of this judgment will be a reconsideration of the current terms of NIPS documentation and procedures relating to the interception and monitoring of prisoner communications. It is clear from some of the submissions made in this case that the contents of some of these would benefit from revision and updating in any event. (For instance, the excerpts of the Security Manual provided refer in a number of places to rule 67 where, since amendments have been made to the Prison Rules, it should now refer to rule 68A. In addition, in a number of documents, the effect of rule 68A(5) is obviously not reflected, adequately or at all. The random nature of what I have referred to as residual monitoring, in respect of both calls and letters, could also be made more clear in the compact.) In my view, there is much to be said for the applicant's basic point that the level of information published in this regard by HM Prison and Probation Service in England & Wales is an example of good practice.