CO/1052/2017

IN THE HIGH COURT OF JUSTICE
QUEEN'S BENCH DIVISION
ADMINISTRATIVE COURT

BETWEEN:

THE QUEEN on the application of
LIBERTY

Claimant

-and-

(1) THE SECRETARY OF STATE FOR THE HOME DEPARTMENT
(2) THE SECRETARY OF STATE FOR FOREIGN AND COMMONWEALTH AFFAIRS

Defendant

SECOND WITNESS STATEMENT OF ANDREW SCURRY

I, Andrew Scurry of the Home Office, 2 Marsham Street, London SW1P 4DF, will say as follows:

1. I am Head of the Investigatory Powers Unit in the Home Office. I have held this position since March 2016. I am responsible for the policy and legislation concerning investigatory powers, including communications data, and was involved in the policy development, parliamentary process and implementation of the Investigatory Powers Act 2016 ("The Act"). I make this second statement on behalf of the Defendants. The purpose of the statement is to address an issue given some prominence before the Court today as to the timing of the introduction of independent authorisation for communications data access requests, and in particular the time taken to establish the Office for Communications Data Authorisations ("OCDA"), the independent body charged with the prior authorisation of requests for access to retained data.

2. In my first witness statement, signed on 19 December 2017, I stated that OCDA was anticipated to begin considering applications from summer 2018 (paragraph 90, p.225 of the bundle). That was also the view set out in the Impact Assessment of 26 November 2017 which was produced to the Court by the Claimant today.

3. The Defendants' skeleton, served on 19 February 2018, stated upon instruction that the Defendants' best current estimate of the time by which the prior authorisation regime could

be brought into operational effect is 1 April 2019. Various reasons were given for that, set out in paragraphs 15-18 of the skeleton. The point made in court today was that this position had not been set out in evidence. Given the importance of the question of the length of any suspension of disapplication, this statement provides in evidence confirmation of the position set out in the skeleton argument and some brief further explanation and context for the time frame set out in it.

4. OCDA will be authorising approximately 200,000 access requests per annum from around 600 public bodies. In order to establish the OCDA authorisation regime, operating effectively with existing systems for data management, it is necessary to do the following.

5. First, OCDA needs to ensure that its IT systems are fully integrated with the array of systems currently used by police forces (and other non-police users) for managing communications data applications.

6. The way in which communications data applications work is as follows:

   (1) An officer within the relevant public authority will fill out an application form.
   (2) The application form will go to a Single Point of Contact ("SPOC") within the authority.
   (3) The SPOC will check the application, to assess whether it is consistent with the law and to advise on whether it is likely to meet the tests of necessity and proportionality.
   (4) The SPOC will then send it to a senior officer (a designated person of sufficient rank), who will himself formally consider necessity and proportionality, and decide whether to authorise the application.
   (5) The senior officer will send the application back to the SPOC.
   (6) The SPOC will liaise with the communications services provider to obtain the data; and
   (7) The data will be provided to the officer making the application.

7. IT systems for managing communications data applications will regulate this entire process, to ensure that it runs smoothly and errors are avoided. The Interception of Communications Commissioner was understandably very keen to ensure that systems of this type were used.

8. OCDA will need to interact with more than 80 public authorities with bespoke IT systems for managing their communications data authorisations. Among the different police forces

alone, there are currently 29 different versions of the 3 systems (developed by 3 different companies) which regulate the above process, up to a security classification of "Official Sensitive". Applications above that (i.e. for Secret or Top Secret material) use a number of further "bespoke" IT systems, with particular access requirements (for example, the terminals need to be in a secure environment, with "bespoke" cabling).

9. OCDA will replace the final authorising person within the above authorisation process with its own independent authorisation procedure. So it needs access to every one of the IT systems concerned, and needs its own IT systems to be consistent with them. I note too that each of those IT systems will itself need to be updated so that it is consistent with the Act rather than RIPA.

10. This IT integration is a really significant task. It is probably the most difficult part of setting up OCDA. If OCDA were to take shortcuts, and try to work around the above requirements (for example, by not using the existing systems for managing communications data applications), it is highly likely that there would be an increase in errors which infringed individuals' privacy rights (for example, data relating to an incorrect phone number being accessed because of a figure being typed wrongly). Anything that does not involve an existing automated system is more likely to generate errors.

11. Secondly, OCDA also needs to recruit approximately 100 staff, who will then need to undergo appropriate training and obtain relevant security clearances. It will also be necessary for the thousands of staff currently employed by public authorities involved in acquiring communications data to undergo training in relation to new processes.

12. Thirdly, OCDA needs to obtain suitably located accommodation, capable of securely handling and storing highly sensitive material, including material classified as Top Secret, and carrying out any necessary works to install appropriate secure networks (which may involve, e.g., obtaining permission from the Highways Agency to carry out works). That will include cabling for the necessary secure networks (in other words, digging up the road to install the appropriate cabling).

13. Many of the above steps entail resolving and agreeing issues with all the public authorities concerned, and a number obviously cannot be taken concurrently, but only sequentially.

Deciding where OCDA should be located is the first step. This has not been easy, because of associated security requirements. Premises have now been identified, and we expect a final decision of the Investigatory Powers Commissioner (Lord Justice Fulford) shortly. The next step will be to advertise, recruit and train staff, and obtain the relevant security clearances. This will take a number of months, for obvious reasons. Before they are trained, OCDA needs to know what IT systems it is going to be using: they will need to be trained on the IT system they are actually using (indeed, before the training can be designed, let alone delivered).

14. The work and the planning are in progress; and estimates of realistic timescales have developed. As we have looked in more detail at what the IT requirements are, and understood fully how many different systems there are and what their separate requirements are, and as the planning of sequencing has developed, it has become clear that the initial estimate of the anticipated start date is impossible to achieve. Those detailed plans have only been finalised this month, and agreed with Lord Justice Fulford last week. Lord Justice Fulford has indicated that in his view April 2019 is the earliest practicable date for implementation of OCDA, as appears from the letter I exhibit to this statement.

I believe that the facts in this witness statement are true:

Signed: [redacted]

Dated: 28/02/18

IPCO
Investigatory Powers Commissioner's Office

PO Box 29105, London
SW1V 1ZU

Letter from the Investigatory Powers Commissioner

27 February 2018

The date of commencement for the independent body which will consider data requests

On 11 September 2017, at the Home Secretary's request, I accepted responsibility for the independent body that will consider requests for access to retained data as forming part of my role as the Investigatory Powers Commissioner. This was on the basis that certain conditions were accepted:

i) Provision of appropriate accommodation.

ii) Provision of a sufficient number of trained/experienced staff to deliver an effective and efficient service as set out in the model produced by the project team.

iii) Provision of a budget.

iv) Access to the Home Office's Human Resources, Estate Management, Information Technology and Financial Services business functions.

v) Provision of an appropriate IT solution to allow the effective exchange of applications/authorisations between the OCDA and public authorities.

vi) Appointment of an interim Chief Executive of OCDA to facilitate development and implementation.

Those conditions give a flavour of the scale of the task that I was fully aware would confront this new organisation, albeit a considerable amount of work had been undertaken before my appointment. Once my interim Chief Executive (Shainila Pradhan) was able to take up her post on 18 October 2017, the pace of implementation increased. I am writing, therefore, from the perspective of someone who has been engaged with this project for less than 6 months.

As the judge with responsibility for this endeavour, I write in support of the submission that the Court grants a stay until April 2019 before the new body (to be called the Office for Communications Data Authorisations "OCDA") begins work. The detailed planning, as set out above, is underway in earnest, but this work has exposed the complexity and challenge of delivering an independent organisation that will consider applications for access to communications data. I am aware that Andrew Scurry will address the detail of the difficulties that confront OCDA in a separate witness statement, and I will therefore confine my remarks to a few general observations.

It is important that the new body is established as a sustainable independent organisation. Any attempt to rush the complex work that needs to be undertaken will significantly increase the risk that errors will occur that could significantly undermine the new regime's efficiency and effectiveness, and which will put at jeopardy its ability to deal with the applications in a secure manner.

The initial plans that had been developed led to the previous suggested date for the establishment of OCDA of July 2018. However, the true extent of the task that needs to be undertaken has only been revealed as the planning has developed and a multiplicity of difficult issues have been identified. Following approval at the relevant Board, I was first presented with the detailed and properly articulated implementation plans on 21 February 2018. I am entirely satisfied that these plans are robust and that the conclusion that OCDA cannot be established before April 2019 is sound.

I will continue to scrutinise this developing work with care, and to encourage my team and the relevant external officials to accelerate the process of implementation. However, I do not believe the previous estimated date of July 2018 is achievable; indeed I am extremely concerned that the new body would be faced with a disastrous beginning if it is maintained.

I greatly regret the continued delay, but I consider the revised date of April 2019 is achievable and gives an appropriate (yet not in any sense over generous) length of time to establish a robust organisation.

With best wishes,

[redacted]

Lord Justice Fulford