POL00139652

CONFIDENTIAL AND LEGALLY PRIVILEGED
POST OFFICE GROUP LITIGATION
17 July 2019

WOMBLE BOND DICKINSON

Decision paper: Preservation of data stored on Post Office's File Servers

1. EXECUTIVE SUMMARY

1.1 Post Office is currently hosting old file server data, the majority of this has not been accessed for more than 2 years, but it costs around £4.4k per month to host. In compliance with Post Office's data retention policies this data should be deleted however consideration is being given as to how this data is preserved for the purposes of the Group Litigation.

1.2 To seek to preserve the data, a copy has been taken which will be held by Consilio (e-disclosure provider). Before the original data is deleted, steps have been taken to seek to obtain confirmation that 100% of the data has been copied. Through this analysis it has been possible to confirm a 99.6% match. For the remaining 0.4%, manual spot checks have been undertaken to seek to confirm whether this data could be found.

1.3 Post Office IT's recommendation is that the data can be deleted and believe that the evidence provided is strong enough that the risk of any actual data loss having occurred is extremely low.

1.4 This paper is seeking Steering Group input into the recommendation to delete this data.

2. BACKGROUND

2.1 As part of the DXC Exit Project, Post Office is looking to delete the data which is held on its File Servers. The File Servers hold data which is saved on the mapped driver letters which are accessible through Post Office employee's laptops. The File Servers contain a mixture of documents, some of which need to be preserved from the purposes of the Group Action.

2.2 The project has already identified that 90% of the data held on the File Servers had not been accessed for more than two years and the majority was transferred from personal drives during the migration to Office 365 and was therefore last accessed when the data was transferred from DXC's northern to southern data centres two years ago. Post Office is now looking to delete the data held on these servers and rely upon a copy which has been taken for the purposes of preserving documents for the Group Action.

2.3 This paper seeks a decision on whether the data should be deleted or maintained for the duration of the Group Action.

3. THE PROCESS

3.1 In order to obtain a copy of the data contained on the Post Office servers, we understand Accenture followed the below methodology:

3.1.1 Original data from Post Office's servers was copied using Robocopy to a new location – the data amounted to c. 9.5 TB of compressed zip files.

3.1.2 Robocopy logs were reviewed by Post Office IT for errors/skipped files. Robocopy logs contain details of a file copy from the source (server) to the destination. It logs all files/folders it is instructed to copy from the source.

3.1.3 Robocopied data was placed into Zip files and copied onto a NAS Drive.

POL00139652

3.1.4 NAS Drive containing the Zip files was shipped to Consilio for verification (e-discovery provider).

3.2 Consilio have undertaken a number of checks to confirm that the data extracted and copied to the NAS Drive matches the data stored on the servers and that the data remains accessible. An explanation of the steps taken is set out below.

3.3 Whilst Post Office can take some comfort from the checks and validations, we as lawyers cannot confirm whether there have been any issues with the data migration or whether there will be any issues with accessing the data going forward as these are technical questions.

Review of Robocopy logs - skipped / failed files

3.4 A copy of the Robocopy logs, created during the copy process by Post Office IT, was provided to Consilio for review. A review of the Robocopy logs highlighted a number of issues with the data copy. We understand from Consilio that it is not unusual that files/folders fail to copy. This could be due to permissions issues (where the Robocopy operator does not have permission to access specific files/folder), files being open, or other reasons, such as documents being deleted during the course of the copy.

3.5 The issues identified by Consilio with the copy were:

3.5.1 skipped directories (37 in total) – Post Office IT has confirmed that the skipped directories were documents located in the recycle bin which failed to copy.

3.5.2 failed files (9,642 in total) – Post Office IT has confirmed that the failed files were documents which were deleted whilst the copy was in progress.

3.5.3 failed directories (732 in total) - Post Office IT has confirmed that the failed directories were documents which were deleted whilst the copy was in progress.

Details of the failed files/directories are set in the below spreadsheet.

917090_Robocopy_Errors_External.xlsx

Comparison of Robocopy logs to data on NAS Drive

3.6 A further check was also undertaken in comparing the Robocopy logs to the data provided to Consilio on the NAS Drive. A log of the data on the NAS Drive was generated and a comparison of this log to the Robocopy logs was run.

3.7 In summary, the comparison confirmed that 99.6% of the original data had been copied onto the NAS drive, and matches were not found on the drive for the remaining 0.4% of data. It does not follow from this conclusion that the data is not contained on the NAS Drive, since there could be other reasons for the comparison not working (ie. file names not matching). The outcome of this comparison is set out below.

Robocopy Log	Total Files from Robocopy Log	Files Found	Not Found
MDS01.log	2,202,230	2,185,084	17,146
MDS02.log	6,570,494	6,522,595	47,899
MDS03.log	6,416,755	6,402,841	13,914

POL00139652

MDS04.log	3,280,943	3,272,847	8,096
MDS05.log	4,435,233	4,429,302	5,931
MDS06.log	3,410,537	3,397,829	12,708
Totals	**26,316,192**	**26,210,498 (99.6%)**	**105,694 (0.4%)**

3.8 As part of this review it was noted that the provided Robocopy logs appeared to have been created using the /LOG command, not the /UNILOG command. As such special characters (£, @, €, etc.) were not maintained and therefore the comparison did not find matches for documents where special characters had been removed – this has increased the volume of files not found. Enquiries were made as to whether it was possible to recreate the Robocopy logs with the correct command so that the comparison could continue. This was not possible as the data was still active and users had been accessing the servers since the first copy was created.

3.9 A further verification was therefore undertaken whereby Post Office selected a number files from the 0.4%. Consilio then sought to verify if: (1) the files existed on the NAS Drive, (2) the files could be restored without issue, and (3) the restored files were accessible. Post Office provided a list of files and a search was undertaken in the data held by Consilio for these. The results of this exercise are set out below. In summary, 11% of the files could not be verified.

Robocopy Log	Selected Files from Robocopy Log	Files Found	Not Found	File name different
MDS01.log	69	64	-	5
MDS02.log	13	6	2	5
MDS04.log	12	12	-	-
MDS05.log	1	1	-	-
Total	95	83	2	10
	100.00%	87.36%	2.10%	10.52%

3.10 Where the file name is different, it may be that the data is contained on the NAS Drive and matches the file in the original source location however, this has not been confirmed.

Accessibility

3.11 Consilio have also undertaken checks to ensure that the data remains accessible. To do so, Consilio created forensic images of the received data and exported the contents of the drive. There was no indication of errors from the exported data.

4. RISKS OF DELETING THE DATA

4.1 The cost of continuing to host the data is around £53k for a further 12 months (circa. £4.4k per month). This needs to be weighed up against the risk of deleting the data.

POL00139652

4.2 Parties to litigation must take reasonable steps to preserve documents which may be relevant to the matters in issue. Parties are expected to suspend routine document destruction policies when litigation is afoot, although a duty to preserve can be complied with by making copies of sources and documents and storing them. Failure to comply with the court rules on preserving documents could lead to the court drawing adverse inferences if any disclosable documents are destroyed. Some of the data on these servers is relevant to the Group Action and therefore needs to be preserved.

4.3 If the data hosted on these servers is deleted then Post Office would be reliant on the copy of the data held on the NAS Drive being correct. If this copy is not correct, this will cause risks for the Group Action. In light of the criticisms from the Common Issues Trial, whilst this judgment remains in place the disclosure and preservation of documents by Post Office will be under heightened scrutiny. The ongoing attitude of the Judge is that anything that looks like Post Office failing to preserve materials is likely to be heavily criticised. Adverse inferences could be drawn that Post Office is hiding something and risks feeding into the Judge's current perception of Post Office.

4.4 If the preservation of this data is challenged in the litigation, a member of Post Office IT, Accenture and Consilio may need to provide witness statements explaining what happened. We may also require a further witness statement from a senior employee explaining why the decision to delete the data was made.

5. OPTIONS

5.1 This is ultimately a business decision on whether Post Office is willing to accept the litigation risks vs. the ongoing costs of hosting.

5.2 Post Office options are:

5.2.1 Option 1 - Delete the data from the server and rely upon the copy of the data on the NAS Drive.

5.2.2 Option 2 - Continue to host the data for a further 12 months.

5.2.3 Option 3 - Due to the format/encoding of the provided Robocopy logs, it is not possible to reconcile all the errors. Two alternatives would be to either recollect using a verifiable forensic tool, or for PO to recollect using a backup solution available to them which has suitable logging and maintains metadata.

5.2.4 Option 4 - Approach Freeths to seek agreement that they are satisfied that the migration has been carried out effectively and that Post Office can rely on the copy of the data on the NAS Drive.

5.3 If Option 1 is followed, we recommend producing and signing witness statements from the relevant individuals before the data is deleted.

5.4 If Option 2 is followed, we recommend re-assessing this decision in 12 months' time when the landscape of the litigation has evolved.

5.5 Option 3 will require the above work to be re-undertaken at additional costs and may not result in a verification that all of the data has been copied. This approach is not recommended.

5.6 If Option 4 is followed, we recommend obtaining a formal report from Consilio to give assurances to Freeths. If Freeths agree to the deletion of the data this would provide Post Office with the maximum level of protection, although not complete as the Judge may still raise concerns in any event. However, it is unlikely Freeths would agree to Post Office deleting the data. In these circumstances, Post Office will still need to make a decision of whether to delete

POL00139652

or retain the data, with the additional factor that Freeths have objected to the deletion. For this reason, we would not recommend this approach.

6. RECOMMENDATION

6.1 Our recommendation is to adopt Option 1, as the commercially balanced approach, but Post Office would need to accept the risk of future challenges in Court in the unlikely circumstances that a material documents has gone missing and is not held on the NAS Drive.