Neutral Citation Number: [2017] EWHC3113 (QB)

Case No: HQ15X05099

IN THE HIGH COURT OF JUSTICE
QUEEN'S BENCH DIVISION

Royal Courts of Justice
Strand, London, WC2A 2LL
Date: 01/12/2017

Before :

THE HONOURABLE MR JUSTICE LANGSTAFF

- -

Between :

Various Claimants	**Claimants**
- and -	
Wm Morrisons Supermarket PLC	**Defendant**

- -
- -

Mr Jonathan Barnes & Ms Victoria Jolliffe (instructed by **JMW Solicitors**) for the **Claimants**
Ms Anya Proops QC & Rupert Paines (instructed by **DWF LLP**) for the **Defendant**

Hearing dates: 9th - 19th October 2017

- -

Approved Judgment

I direct that pursuant to CPR PD 39A para 6.1 no official shorthand note shall be taken of this Judgment and that copies of this version as handed down may be treated as authentic.

.....

THE HONOURABLE MR JUSTICE LANGSTAFF

MR JUSTICE LANGSTAFF :

1. This group action raises the question whether an employer is liable, directly or vicariously, for the criminal actions of a rogue employee in disclosing personal information of co-employees on the web, whether under the **Data Protection Act** 1998, an action for breach of confidence, or in an action for misuse of private information.

2. On 12th January 2014 a file containing personal details of 99,998 employees of the Defendant ("Morrisons") was posted on a file sharing website. Shortly after that, links to the website were also placed elsewhere on the web. The data consisted of the names, addresses, gender, dates of birth, phone numbers (home or mobile), national insurance numbers, bank sort codes, bank account numbers and the salary which the employee in question was being paid. On 13th March 2014, a CD containing a copy of the data was received by three newspapers in the UK, one of which was the Bradford Telegraph and Argus, a newspaper local to Bradford where Morrisons has its head office, The person sending the CD did so anonymously, purporting to be a concerned person who had worryingly discovered that payroll data relating to almost 100,000 Morrisons employees was available on the web. It gave a link to the file-sharing site.

3. The information was not published by any of the newspapers concerned. Instead, the Bradford Telegraph and Argus told Morrisons of it. There was immediate concern. Morrisons' annual financial reports were about to be announced. The revelation of this data, with its implication that Morrisons could not be trusted to keep data secure, had serious implications for the share value of Morrisons. Much more important, though, was the immediate concern of the most senior managers within Morrisons that the information might be used by outsiders to access the bank accounts of individual employees (though they were assured by banks over the next 2 or 3 days this could not happen, without yet more information being disclosed) or used to aid identity theft. It could enable intending fraudsters to phish for the additional information to enable dishonest access to the employees' bank accounts, take out loans, or make purchases under an assumed identity. This was a serious risk.

4. Morrisons' head management was alerted to the disclosure on 13th March 2014. Within a few hours, they had taken steps to ensure that the website had been taken down. Such links as there were to the file sharing website from other sites were then no longer effective in helping a searcher to discover any personal data. Morrisons also alerted the police. It was rapidly established that the data, in the quantity and style in which it was presented, had almost certainly been derived from data held centrally by Morrisons in relation to its employees, both present and, in some cases, past. Only a limited number of employees had been permitted access to the whole of this data, which was held in a supposedly secure internal environment created by proprietary software known as "PeopleSoft". It was possible to tell when the data had been extracted by comparing the disclosed material with the database: the times that entries were made into the database or deletions made from it were automatically logged. Thus, where data now on the database was not amongst that disclosed, this suggested the disclosed data had been extracted beforehand.

5. It was possible by this process to show that the data held in PeopleSoft had been copied during the afternoon of 14th November 2013. It was then also possible to show

that at that time one of the "super users" (the name for people who had access to the whole of the PeopleSoft database, as opposed to having access only to that part which related to them personally or, in some cases, to those employees under their line management) had extracted data corresponding to that disclosed by means of an SQL (structured language query) within the time period during which the data containing the information disclosed must have been copied. This person was Michael Leighton. He was arrested on 17th March 2014.

6. Another employee – an investigator – was also identified as a suspect. This was because his initials and date of birth appeared in the user name adopted for the account which had been used in January 2014 to post the data file onto the internet.

7. It very quickly emerged that Michael Leighton was not responsible for disclosing the file to the web, and that where the initials and date of birth of the investigator had been used this was in a deliberate attempt to frame him. He too was completely innocent.

8. On 19th March, Andrew Skelton, a Senior IT Auditor in Morrisons' employment, was arrested. He was charged with an offence under the **Computer Misuse Act 1990** both of fraud and under Section 55 of the **Data Protection Act 1998**, tried at Bradford Crown Court in July 2015, and convicted. He was sentenced by the Honorary Recorder of Bradford to a term of 8 years imprisonment, which he still serves.

The Claim

9. 5,518 employees of Morrisons whose data was disclosed by the actions of Skelton on 12th January and 13th March 2014 claim compensation both for breach of statutory duty (under Section 4(4) of the **Data Protection Act 1998**) and at common law (the tort of misuse of private information, and equitable claim for breach of confidence). The claims are put on the basis that Morrisons has both primary liability for their own acts or omissions, and secondary (vicarious) liability for the actions of one of their employees harming his fellow workers. In respect of the **Data Protection Act**, primary liability is said to be absolute or strict, rather than a qualified liability only arising if Morrisons failed to observe appropriate standards: but if it should be held that the Act does not impose an absolute liability, it is asserted that in any event Morrisons failed to observe those standards and is liable on that alternative basis.

10. The trial has been concerned only with liability. If the court should find in favour of the Claimants in respect any of their heads of claim, quantum is to be assessed later. Similarly, although in their pleadings the Claimants sought an injunction to prevent Morrisons further disclosing the private and confidential information of the Claimants, and an order under Section 14(4) of the **Data Protection Act 1998** blocking each Claimant's personal data, neither was pursued before me. Accordingly, since most of the facts were not in dispute (having been clarified by the criminal trial and conviction of Skelton) the hearing before me proceeded without any of the Claimants being called to give evidence: they knew little if anything as to how or why the disclosure happened about which they were in a position to give first-hand evidence. That information lay in the hands of Morrisons, and the force of any criticism of what happened, supportive of a case that Morrisons failed to observe applicable standards, depended on evidence called by Morrisons. Accordingly,

Morrisons called evidence from five members of senior management of Morrisons (the evidence of a sixth, Ms Crossland, was taken as read).

11. The parties have agreed that there are 14 issues of fact and law to determine, and set them out in writing. Many of these are themselves subdivided into sub-issues.

The Central Facts

12. I shall first set out an overview of the facts which set the scene for the determination of those issues. Mr. Barnes, with whom Ms Victoria Jolliffe appears for the Claimants, argues that in a number of respects Morrisons fell short of a proper standard (whether under the **Data Protection Act** or common law): I shall deal with my more detailed findings of fact when I consider each of those arguments later in this judgment.

13. There is a statutory obligation resting on Morrisons to have their accounts audited externally. At the times relevant to this action, the external auditor was KPMG. In order to perform the audit, KPMG would, each year, request data so that it could test the accuracy and reliability of the information produced to it. In 2012 (and probably earlier) it asked to have a copy of Morrisons' payroll data so that the integrity of the data could be assessed: payroll expenses are a significant part of Morrisons' accounts. In 2012, amongst various other requests for information KPMG asked for a copy of the "payroll data" being the data from which the data in the file disclosed were copied. This was not the only data requested by KPMG. It was, however, the only data to come from the PeopleSoft system.

14. Morrisons had an internal audit team. At the time of the disclosure, Mr Chowdhery was its head. It had within it an IT audit section. That team was headed up by Graham Daniels, who gave evidence before me. Two or three IT auditors, specifically recruited for the purpose by Mr Daniels, reported to him. One of those was Andrew Skelton ("Skelton").

15. Skelton was a senior IT internal auditor. As such, his role involved speaking to fellow employees about their work and processes, and obtaining sight of relevant documents concerning them. Some of those whose work he had to audit would be more senior than he was. He was given the responsibility and authority to speak to many colleagues and request sight of their documents. He had to exercise diplomacy and sensitivity, and would frequently be expected to gain access to and use information that was sensitive, not only in a business sense, in that it was strictly confidential for internal use only, but also potentially sensitive so far as the colleagues providing the information were concerned. Colleagues had to feel that he was both reliable and trustworthy.

16. As a senior IT auditor, he was highly IT literate, with a good technical understanding of IT security issues, operating systems, user access and cryptography.

17. Unknown at the time to his employers, Skelton operated a sideline in dealing with a slimming drug. He bought quantities, probably in kilograms, from a wholesaler, and re-packaged these in smaller quantities which he offered for sale on e-Bay. He did this in his own time, as a personal business. It has not been suggested that this was in conflict with the business of Morrisons. He did not use Morrisons' facilities, except

on those occasions when, if he had not posted a package to a customer from a post box or office local to his home, he would put the package through Morrisons' post room. When he did so, it had already been appropriately stamped by him. No dishonesty was involved: there was no direct cost to Morrisons.

18. The drug was Phenylalanine, a close analogue to Amphetamine. Whereas Amphetamine is a class B drug, the supply of which is unlawful, the supply of Phenylalanine is not.

19. On 20th May 2013, an envelope he had posted in this way came open in the post room at Morrisons. It contained white powder. This caused immediate alarm to those in the post room, who did not know what the powder was, and who had a protocol for dealing with such incidents. The incident might easily have led to the closure of the post room in accordance with the protocol. The police were called. They suspected the drug might be Amphetamine. A field test at the local police station was indicative of this. Since there was no attempt to hide the identity of the sender, which was mentioned in documents within the package, it was clear that Skelton had sent it. He was arrested and escorted from the premises of Morrisons. He was suspended from work, pending a definitive laboratory analysis of the powder. It took just over a month before the results of that were notified. They showed that the drug was not illegal. Accordingly Skelton, who had been on suspension throughout this period, was permitted to return to work. He did so on 3rd July 2013.

20. However, Morrisons decided to discipline him for the incident, which had caused considerable concern, and might well have led to the closing down of the post room for a day with serious implications for the business. On 9th July 2013 he faced a disciplinary hearing, following which, on 18th July, he was given a formal verbal warning. Though this was described in witness evidence as the lowest level of sanction within the disciplinary procedures, this is not quite so. Morrisons' disciplinary code provided that where after a hearing it was concluded there had been misconduct, possible outcomes began with informal action which is plainly meant to be less serious. It is, however, correct to say that formal actions available to the employer began with a verbal warning, followed by a first written warning, a final written warning, then dismissal on notice for the more serious cases, and summary dismissal for the most serious. It is worth noting for what follows that it is only in the case of dismissal that the code provides for an alternative, lesser, sanction, that of demotion to a lesser position or transfer to an alternative role or department. Though described as a "verbal" warning, the essence of the warning was recorded in writing in a letter written formally to Skelton, as was the practice. It was to stay on his file for six months.

21. Skelton was unhappy that he had been given a formal, albeit "verbal", warning, and said as much to his line manager Graham Daniels. Mr Daniels thought that Skelton had been irritated by the fact he was given such a low level of sanction, since this reinforced his (Skelton's) view that Morrisons' initial reaction to the incident had been excessive, even though he (Skelton) understood that a disciplinary process had been warranted. He thought the sanction disproportionate, and exercised his right to appeal. The appeal came before Ms Joanna ("Jo") Goff on 15th. August 2013 and was rejected. The disciplinary decision recited that Skelton's actions had not been in accordance with Morrisons' values. Those values are set out in a handbook given to all employees. There are 6 of them: "Can Do"; "One Team"; "Bringing the Best out

of our People"; "Great Selling and Service"; "Great Shopkeeping"; and "Fresh Thinking".

22. At his trial Mr Skelton denied being responsible for the data disclosure. He did not advance any reason for having acted as he did. However, the Recorder of Bradford had no doubt that it was the white powder incident which caused Skelton to do as he did. When sentencing Skelton on 17th July 2015 he said:

> "[the white powder incident]… was concluded against you, not that in fact there was anything particular that happened by way of discipline of you. One would think that any sensible, reasonable person would have just put that behind them and got on with life and got on with their job. That was not your reaction. Your reaction was to harbour a very considerable grudge and harbour very considerable bad feelings towards Morrisons. That much is evident if nothing else, from the resignation letter that you drafted in November of that year, a few months after the incident and disciplinary proceedings had been concluded. It was rankling very deeply and nastily with you.
>
> Your reaction was to set about, in October or November, doing Morrisons some real damage, and you achieved that of course. Over a period of months at the end of the year you set about getting sensitive information from Morrisons – it came legitimately into your hands, trusted as you were in that IT department – the pay roll details and personal details of all the employees at Morrisons, who of course number over 100,000. Having got hold of that material legitimately at work you took it away from work electronically and you, in November and December – so over a period of weeks, not just on the spur of the moment – started to set up what you put into effect in 2014. You created a false email account, you got a pay as you go mobile telephone that could not [be] traced back to you, you started to use the TOR system which we heard about which is a way of seeking and achieving anonymity in terms of what you were to do on the internet. …it was cold and calculating and designed, no doubt, to do as much damage to Morrisons as could be achieved."

23. Not only did His Honour Judge Thomas QC, the Honorary Recorder, have the benefit of hearing the evidence in the criminal trial which included that of Skelton himself, such that I would in any event pay great respect to his conclusions, but these findings are also entirely consistent with the documentation before me.

24. On 9th October 2013, unknown to Morrisons, Skelton made a search for "TOR" on his work computer. The acronym stands for "The Onion Router": software which is capable of disguising the individual identity of a computer which has accessed the internet.

25. On 1st. November, the external auditor, KPMG, requested a number of categories of data from Morrisons. This was held in different places. It was convenient that the data be collated before transmission to KPMG. The request came to Mr Daniels. In previous years Mr Daniels had been charged by Mr Chowdhery, head of the team, with arranging for the transmission of such data to the external auditor. Mr Daniels delegated the task in 2013 to Skelton, one of the two or three internal auditors who reported to him, just as he had delegated an identical task to Skelton (I find) in 2012. Skelton in turn sent an email request to Dan Moore of the HR department, who had super-user access to PeopleSoft. He in turn delegated the task of extracting a copy of the data, by means of an appropriate SQL query, to Michael Leighton. On 14th November, Michael Leighton obtained an electronic copy of the data. This was in the late afternoon. He attempted to email the data internally to Skelton. I find that the transfer would have been secure if the internal email system had been able to cope with the transfer of a data file of that size. It was not. So, although Michael Leighton completed documentation suggestive that the transfer had been effective on 14th November 2013, in fact the email "bounced back" to Michael Leighton's computer. Accordingly, the next day Michael Leighton copied the data from his computer onto a USB stick. Insofar as it is in issue I find that the USB was encrypted (personal USB sticks were not to be used; a limited number of USB sticks were made available to senior employees, obviously for the transfer of data, and all were encrypted; the overwhelming probability is that Michael Leighton used one of these, and there is no reason to suppose otherwise). He took the USB stick personally to Skelton at his laptop computer, which was itself encrypted. He was present while the data was downloaded from the stick onto the computer and he then returned with the USB stick to the (nearby) desk from which he had come.

26. Skelton was supplied with a separate USB stick, from KPMG, encrypted by it, onto which he later copied the data. He had the task of collating the payroll data and other data which had been requested by KPMG, which was not itself held on the PeopleSoft system. For that reason, the payroll data was not sent immediately to KPMG, but remained stored for the time being on Skelton's computer. The precise date on which Skelton provided the pay roll data to KPMG on a KPMG USB (together, I assume, with the other data he had collated) is not known. It must, however, have fallen between the 15th November (when he, Skelton, was supplied by Leighton with the data) and 21st November.

27. On 18th. November 2013 it is agreed by the parties that an unknown USB device was inserted into Skelton's work laptop. Various files which included the pay roll data and the file later uploaded to the file sharing website (which was termed the "FTSE 100" file) were deleted from the same USB on the 12th. March 2014, using Skelton's personal computer to do so. From this, limited, material, coupled with the knowledge (it is agreed as fact) that on 14th November Skelton obtained the mobile phone he was later to use to facilitate the offending data disclosures, I infer that Skelton copied the payroll data onto a personal USB at work on 18th. November 2013, and that this was a step in his criminal conduct. Given that in December the phone was registered with an email address implicating the innocent investigator, and that it was not used until the 12th. January when uploading data to the web, I infer that Skelton – who would have known from his previous year's experience what type of data he would be dealing with – had it in mind from before the 14th. November to misuse that data.

28. The next incident of note before the uploading of the data to the file-sharing website was on 16th. December 2013. Skelton attempted to access the TOR website from his work laptop. This was unknown to Morrisons until after it had come to light that the employee details had been placed in a file on a file sharing website and copied to national and local newspapers, on respectively 12th. January and 13th. March 2014.

29. No point arises for decision in respect of Morrisons' reaction to the disclosures once it knew of them.

30. Each employee had supplied the information later disclosed because it was required by Morrisons upon that employee taking employment with them.

The Claimants' Case

31. So far as direct, primary, liability is concerned, the Claimants made claims under the **Data Protection Act 1998**, under common law for misuse of private information, and in equity, for breach of confidence. If Morrisons were not held primarily liable, the Claimants submitted they were liable vicariously, under each of the three heads. I shall deal with each of the claims in turn, beginning with the claims of primary liability.

32. Ms Proops argued that there could be no primary liability for breach of confidence, for Morrisons itself did not breach the confidence.

Data Protection Act 1998

33. The **Data Protection Act (the "DPA")** provides, so far as material as follows: By section 1 (headed "Basic interpretative provisions"):

> "(1) In this Act, unless the context otherwise requires—
>
> "data" means information which—
>
> (a) is being processed by means of equipment operating automatically in response to instructions given for that purpose,
>
> (b) is recorded with the intention that it should be processed by means of such equipment,
>
> (c) is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system,
>
> (d) does not fall within paragraph (a), (b) or (c) but forms part of an accessible record as defined by section 68; ….
>
> "data controller" means, subject to subsection (4), a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed;

"data processor", in relation to personal data, means any person (other than an employee of the data controller) who processes the data on behalf of the data controller;

"data subject" means an individual who is the subject of personal data

"personal data" means data which relate to a living individual who

can be identified—

(a) from those data, or

(b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller,

and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual;

"processing", in relation to information or data, means obtaining,

recording or holding the information or data or carrying out any operation or set of operations on the information or data, including—

(a) organisation, adaptation or alteration of the information or data,

(b) retrieval, consultation or use of the information or data,

(c) disclosure of the information or data by transmission, dissemination or otherwise making available, or

(d) alignment, combination, blocking, erasure or destruction of the information or data;

(2) In this Act, unless the context otherwise requires—

(a) "obtaining" or "recording", in relation to personal data, includes obtaining or recording the information to be contained in the data, and

(b) "using" or "disclosing", in relation to personal data, includes using or disclosing the information contained in the data.

(3) In determining for the purposes of this Act whether any information is recorded with the intention—

(a) that it should be processed by means of equipment operating automatically in response to instructions given for that purpose, or

(b) that it should form part of a relevant filing system,

it is immaterial that it is intended to be so processed or to form part of such a system only after being transferred to a country or territory outside the European Economic Area.

……"

34. By section 4 is provided, under the heading: "The data protection principles"

> "4.—.
>
> (1) References in this Act to the data protection principles are to the principles set out in Part I of Schedule 1.
>
> (2) Those principles are to be interpreted in accordance with Part II of Schedule 1.
>
> (3) ……..
>
> (4) Subject to section 27(1), it shall be the duty of a data controller to comply with the data protection principles in relation to all personal data with respect to which he is the data controller."

35. Part I of Schedule 1 states, so far as relevant:

> **"SCHEDULE 1**
>
> **The data protection principles**
>
> **PART I**
>
> **The principles**
>
> 1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless—
>
> (a) at least one of the conditions in Schedule 2 is met, and
>
> (b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.
>
> 2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
>
> 3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
>
> 4. Personal data shall be accurate and, where necessary, kept up to date.

5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

6. Personal data shall be processed in accordance with the rights of data subjects under this Act.

7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data."

35. The data protection principles are expanded by Part II of Schedule 1 as follows (again, so far as material):

> *"The first principle*
> **1.—**
> (1) In determining for the purposes of the first principle whether personal data are processed fairly, regard is to be had to the method by which they are obtained, including in particular whether any person from whom they are obtained is deceived or misled as to the purpose or purposes for which they are to be processed.
> ……
>
> **2.—**
> (1) Subject to paragraph 3, for the purposes of the first principle personal data are not to be treated as processed fairly unless—
> (a) in the case of data obtained from the data subject, the data controller ensures so far as practicable that the data subject has, is provided with, or has made readily available to him, the information specified in sub-paragraph (3), and
> (b) in any other case, the data controller ensures so far as practicable that, before the relevant time or as soon as practicable after that time, the data subject has, is provided with, or has made readily available to him, the information specified in sub-paragraph (3).
> ……
>
> (3) The information referred to in sub-paragraph (1) is as follows, namely—
> (a) the identity of the data controller,
> (b) if he has nominated a representative for the purposes of this Act, the identity of that representative,
> (c) the purpose or purposes for which the data are intended to be processed, and
> (d) any further information which is necessary, having regard to the specific circumstances in which the data are or are to be processed, to enable processing in respect of the data subject to be fair.
> **…….**

> *The second principle*
> **5.**
> The purpose or purposes for which personal data are obtained may in particular be specified—
>
> (a) in a notice given for the purposes of paragraph 2 by the data controller to the data subject, or
> (b) in a notification given to the Commissioner under Part III of this Act.
>
> **6.**
> In determining whether any disclosure of personal data is compatible with the purpose or purposes for which the data were obtained, regard is to be had to the purpose or purposes for which the personal data are intended to be processed by any person to whom they are disclosed.
>
> **……**
>
> *The seventh principle*
> **9.**
> Having regard to the state of technological development and the cost of implementing any measures, the measures must ensure a level of security appropriate to—
>
> (a) the harm that might result from such unauthorised or unlawful processing or accidental loss, destruction or damage as are mentioned in the seventh principle, and
> (b) the nature of the data to be protected."

36. As to the consequence of any breach of the duty to observe these principles, section 13 provides:

> "13.— Compensation for failure to comply with certain requirements.
>
> (1) An individual who suffers damage by reason of any contravention by a data controller of any of the requirements of this Act is entitled to compensation from the data controller for that damage.
>
> ……..
>
> (3) In proceedings brought against a person by virtue of this section it is a defence to prove that he had taken such care, as in all the circumstances, was reasonably required to comply with the requirement concerned."

37. Of relevance to the present claim is that data is "information": it is plain that a principal thrust of the Act concerns data electronically held, as was the information in respect of the employees' identities as set out above. What is important for what follows are the definitions of "data controller", "data processor" as set out above, and

Section 1(2) which provides that unless the context otherwise requires "disclosing" in relation to personal data, includes disclosing the information contained in the data.

38. The Claimants argue that Section 4(4) places a duty on a data controller to comply with the data protection principles in relation to all personal data with respect to which he is data controller. Here, the Claimants say Morrisons were at all relevant times the data controller in respect of the payroll data abstracted from PeopleSoft by Michael Leighton and transferred to Skelton. They assert that Morrisons did not comply with data protection principles 1, 2, 3, 5 and 7.

39. For DPP1 to be satisfied certain conditions are to be met before the data may be regarded as being processed fairly and lawfully. The first of those conditions, to be found in DPA schedule 2, is that the data subject has given his consent to the processing. That did not happen, because none of the Claimants consented to Skelton processing the data by copying it, processing the original data so as to produce an extract of the information of which the original data consisted, and then sending that extract to the file sharing website.

40. They claim, too, that DPP2 was not complied with because the data was processed not only for administration, payroll and audit purposes, but for the criminal purposes known only to Skelton. They assert that what happened was thus processing in a manner incompatible with the purposes for which the data was obtained from them.

41. DPP3 requires that "personal data are not excessive". Beyond complaining that this principle was broken, the Claimants' argument in court did not further amplify the way in which the data they provided to Morrisons was "excessive": on the face of it, it was exactly the sort of payroll information which almost any employer is likely to require, and then to hold. Only a little more was said as to the claim in respect of DPP5 - that personal data are not to be kept for longer than necessary for the purpose or purposes for which they have been obtained. Insofar as Morrisons were concerned, it was thought necessary to keep the information in the hands of Skelton, as Morrisons thought securely, for a short period after transfer to KPMG: there might need to be queries raised, which it would be easier and more efficient for Skelton to answer from the material stored on his work laptop rather than have once again to request a superuser to conduct an SQL request to identify the data again, and transfer it once more to him. I accept the Defendant's evidence that if the system had required such requests and answers it would have incurred the additional risk inherent in any transfer of data out of the secure environment of PeopleSoft to a laptop, even if encrypted. I find that to do as was done was thus, if marginally, the safer option.

42. Although Section 13 of the Act provides that it will be a defence (the burden of proving which rests upon the Defendant) to show that all reasonable care was taken by the Defendant to satisfy the data protection principles, the Defendants have not relied upon this defence. In the absence of their doing so, there could be no defence to a claim if it were shown that any of DPP1, 2, 3 or 5 were broken. As to DPP7, there would be a breach if there were a failure to apply appropriate technological or organisational measures to prevent the disclosure or loss in question. It is thus necessary to determine what the scope of "appropriate" measures are, an inquiry necessarily related to the particular facts of the particular case.

43. Ms Proops QC, who appears with Mr Paines for Morrisons, makes a case that they do not need to avail themselves of the defence in section 13 to avoid primary liability. This is because the structure of the Act places the responsibilities created by DPP1-8 upon the data controller, as defined. She argues that data is not the same as "property". It consists of information: information is not the same as property. If information is seen and copied, it is not sensible to talk of the information as having been "stolen": unless it is deleted at the same time as it is copied it remains on the database from which the information was extracted. At any one time there may be many sets of data containing precisely the same information. In **Your Response Ltd v Data Team Business Media Ltd** [2014] EWCA Civ 281, it was held that the concept of possession in the conventional sense had no meaning in relation to intangible property, and it was thus not possible for a lien to exist over an electronic database. At paragraph 42 of the judgment Floyd LJ noted that although information may give rise to intellectual property rights the law has been reluctant to treat information itself as property. The court declined to do so in the case before it; in the words of Moore-Bick LJ (paragraph 19) the process of entering information into an electronic data storage system:-

> "…does not in my view render the information itself a physical object capable of possession independently of the medium in which it is held and in the electronic world the distinction is of some importance because of the ease of making and transmitting intangible copies."

44. This conceptual understanding of information as being distinct from tangible property helps to explain the way in which the **Data Protection Act 1998** is structured. The duties under section 4, and generally within the Act, are imposed upon a data controller, even if a third party may be guilty of a criminal offence under section 55 of the Act as was Skelton here. In **Ittihadieh v 5-11 Cheyne Gardens RTM Company Ltd** [2017] EWCA Civ 121, in the course of considering a case which centred upon the law relating to subject access requests under the DPA, the court had to decide (as an issue) the scope of the definition of "personal data" in Section 1 of the DPA, and the question who was a "data controller" (see paragraph 1(i) and (ii) of the judgment). In a judgment with which Lloyd-Jones and McCombe L.JJ agreed Lewison LJ said at paragraph 70 and 71, under the heading "who is a data controller?" as follows:

> "70. A data controller is a person who makes decisions about how and why personal data are processed. It is clear from the terms of section 7(1)(a) that the data controller is responsible for persons who process data on his behalf. Thus it follows that a person who processes data as agent for a data controller is not himself a data controller in respect of those data. Even where decisions about data are taken by natural persons, they will not themselves be data controllers if those decisions are made as agents of a company of which they are directors: *Re Southern Pacific Personal Loans Ltd* [2013] EWHC 2485 (Ch);
>
> 71. On the other hand, if they are processing personal data on their own behalves they will be data controllers as regards

> that processing and those data. The question may then arise whether they are entitled to one or more exemptions under the DPA."

45. Mr Barnes, appearing with Ms Jolliffe for the Claimants, said expressly in closing that he took no issue with the general terms in which those two paragraphs are expressed. Moreover, since the reasoning concerned one of the issues in the case, the view expressed binds me. In any event, I consider it flows from the way in which the Act is structured, and if it had mattered I would independently have been of the same view as the Court.

46. In closing, Mr Barnes thus accepted that if Company A copied data which it held as data controller, and transmitted that copy to Company B, then if Company B did not handle that data in accordance with any one of the data protection principles, Company B would be liable. It would be liable alone, unless it were to process the data for Company A, for it would now be the data controller in respect of the data copied to it: Company A would not. The fact that Company A would remain data controller of the data from which the copy was made would be beside the point. Bringing the example more closely to the facts of the present case, when Skelton transferred a copy of the data he had been given by Leighton from his work laptop onto the USB stick given him by KPMG, and that data was taken to KPMG, KPMG alone were the data controller in respect of the information contained on that data set. Of course, Morrisons remained the data controller in respect of precisely the same information on their own equipment. Mr Barnes accepted that for the purpose of the case in relation to vicarious liability which he sought to advance, he could only do so under the DPA if Skelton were a data controller, in respect of the data eventually disclosed on to the web, for only as such would Skelton owe any duty himself which might result in Morrisons having secondary liability for his wrongs. Yet for him to be data controller in respect of that data would put him in no different a position, in my view, from the position occupied respectively by Company B or KPMG in the two examples just given.

47. Ms Proops' submissions are entirely in line with this approach. She submits that Morrisons owed duties under Section 4(4) DPA only while data controller, and only qua data controller. Skelton became data controller in respect of that information once he put himself in the position of determining the purposes for which and the manner in which the personal data he was about to copy from his laptop was to be handled. When he decided to settle his grudge against Morrisons by means of disclosing it, eventually, on the internet, he was acting just for himself. He was in the same position as the hypothetical individual considered in paragraph 71 of **Ittihadieh**.

48. Mr Barnes argues that if a data controller may only be held liable if **it** has contravened its statutory obligations under the DPA, Ms Proops' analysis would have a data controller complying with the DPA through the actions of its employees, but never being in breach of its obligations should an employee misuse data. He submits this would make a nonsense of the statutory scheme, for a data controller could simply disown any act of its employee which if attributed to it would put it in breach of statutory duty. Instead, to be effective the statutory scheme itself should impute to a non-natural data controller the data processing actions (good or bad) of its employees.

49. I cannot accept this. Not only do I see no reason why, if it is sound, the principle should not apply to natural persons as well as corporate bodies, for both may have employees, and both may act through them, but at its heart is the contention that upon its true construction the Act imposes liability on a data controller not only for those breaches it has authorised or facilitated (acting, if a corporation, by individuals to do so) but also for those it has neither facilitated nor authorised. Indeed, it may have taken great pains to avoid doing so. If a corporation (or individual) is to be liable for breaches which it is in no sense responsible for either authorising or requiring, but which are committed by employees acting in contravention of its wishes, that liability may be established vicariously - but not directly.

50. Untrammelled by the question whether the European origins of the DPA require me to interpret the Statute to hold that when Skelton copied the data unlawfully onto a personal USB stick Morrisons remained primarily liable for this. I would reject the Claimants' case in respect of direct liability under the DPA. I would hold the wording of the Statute, interpreted as it was in **Ittihadieh**, to be such that Morrisons (a) were not the data controller at the time of any breach of DPP1, 2, 3 and 5 in respect of the information later disclosed on the web, and that (b) since they were not the data controller in relation to it owed no duty to the Claimants in respect of which they were in breach, unless it were the duty to comply with DPP7.

51. Although little was said about it during the trial, the fact that the **DPA** was enacted in order to implement a European Directive nonetheless cannot be ignored. A Directive obliges Member States to whom it is addressed to achieve the results it directs. The obligation resting upon a domestic court when interpreting national legislation which implements a Directive is thus to achieve a conforming interpretation: to interpret it "as far as possible" in the light of the wording and purpose of the directive to achieve the result sought by the latter: see **Marleasing v LA Comercial Internacional de Alimentación SA** (1992) 1 CMLR 305, and **Pfeiffer v Deutscher Rotes Kreuz Kreisverband Waldshut eV** [2005] ICR 1307. Accordingly I have to ask whether it requires an interpretation other than that I have already indicated. The linguistic features of the legislation are not conclusive. The effect of interpretation may be to change the meaning of legislation in order to correspond with the purpose of the European law concerned. But the court is not a legislator. There is a critical difference between interpretation on the one hand and legislation on the other. Thus in **Ghaidan v Godin-Mendoza** [2004] 2 AC 557 HL it was accepted that the interpretation chosen by a court must "go with the grain of the legislation" for this would be consistent with the legislative purpose, whereas going against that grain would constitute the court a law maker. Lord Nicholls, Lord Steyn and Lord Rodger all accepted that there would be occasions when the courts could not adopt a conforming interpretation because that would involve making policy choices which the court was not equipped to make. (Though **Ghaidan** concerned the European Convention of Human Rights, it is now well recognised that the principles relating to interpretation in conformity with a Directive are not materially different.)

52. The scope of the Directive, with a view to determining whether section 13 of the DPA was in conformity with it, came for consideration before the Court of Appeal in **Vidal-Hall v Google inc** [2015] EWCA Civ 311, [2016] QB 1003. In the joint judgment of Lord Dyson MR and Sharpe LJ, with which McFarlane LJ agreed, the court rejected an appeal against a decision of Tugendhat J at first instance. There

were two issues – the first whether the cause of action for misuse of private information is a tort (to which I shall return later in this judgment for other purposes) and, the second the meaning of "damage" in Section 13 of the DPA. As for the second issue, the court had necessarily to decide whether the DPA could be interpreted such that "damage" included non-pecuniary loss, such as stress.

53. The Court noted that the DPA was intended to implement Directive 95/46/EC of 24th October 1995, a Directive "on the protection of individuals with regard to the processing of personal data and on the free movement of such data". At paragraph 56 Dyson MR and Sharpe LJ said:

> "The Directive as a whole is aimed at safe-guarding privacy rights in the context of data management. This is repeatedly emphasised in the recitals:
>
> > "(2) Whereas data-processing systems are designed to serve man; whereas they must, whatever the nationality or residence of natural persons, respect their fundamental rights and freedoms, notably the right to privacy, and contribute to economic and social progress, trade expansion and the well-being of individuals;…"
> >
> > …(7) Whereas the difference in levels of protection of the rights and freedoms of individuals, notably the right to privacy, with regard to the processing of personal data afforded in the Member States may prevent the transmission of such data from the territory of one Member State to that of another Member State; whereas this difference may therefore constitute on obstacle to the pursuit to a number of economic activities at Community level, distort competition and impede authorities in discharge of their responsibilities under Community law; whether this difference in levels of protection is due to the existence of a wide variety of national laws, regulations and administrative provisions…
> >
> > …(10) Whereas the object of the national laws on the processing of personal data is to protect fundamental rights and freedoms, notably the right to privacy, which is recognised both in Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms o mom the general principles of Community law; whereas, for that reason, the approximation of those laws must not result in any lessening of the protection they afford but must, on the contrary, seek to ensure a high level of protection in the Community;..
> >
> > …(11) Whereas the principles of the protection of the rights and freedoms of individuals, notably the right to privacy, which are contained within this Directive, give substance to and amplify those contained in the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data…
> >
> > Article 1 provides for the object of the Directive

> "1. In accordance with this Directive Member States shall protect the fundamental rights and freedoms of natural persons and in particular their right to privacy with respect to the processing of personal data." "

54. The Court held that from this material it emerged that the purpose of the DPA was to "provide a high level of protection to the right of privacy in respect of the management of personal data by data controllers". To achieve that purpose, the court considered that Section 13(2) of the Act should be disapplied: the **Marleasing** principle did not permit an interpretation of "damage" which would be consistent with it: a restriction to pecuniary loss, which the use of that word conveyed, was an important element of the compensation provisions that Parliament had enacted. The importance to the scheme of the Act as a whole of the provisions for compensation, in the event of any contravention by a data controller, within the limits set by Parliament to the right to compensation, made them a fundamental feature of the legislation. Yet given the purpose and meaning of the Directive it could only properly be implemented if "damage" permitted non-pecuniary harm, such as distress and loss of autonomy over personal data, to be the subject of compensation.

55. Just as was the case in **Vidal-Hall** where the court had to ask whether it was necessary to interpret the legislative provisions to achieve the purpose of the Directive it had identified and, if they could not be so interpreted, to disapply them, I have to ask in the present case whether it is contrary to the purpose of the Directive to hold that the processing of employee data in a manner unauthorised by those employees is something for which Morrisons is not liable. If it is, I should either find a way of interpreting the DPA to fulfil the purpose, or must disapply the relevant provisions. This is so even if, upon a literal reading of the Act it were to be held that the natural reading of the Act excluded liability where the processing concerned was by the act of a third party, contrary to the desires of Morrisons, nor authorised by it nor by any of its employees in authority.

56. The effect of so holding would, as Ms Proops points out, amount to absolute or strict liability dependent only upon the fact that information supplied to Morrisons had been disclosed subsequently on the internet.

57. I accept both that where an Act of Parliament is the domestic implementation of an E.U. Directive a court should take a purposive approach to the interpretation of that legislation, and that the purpose is that to be found in the Directive. I accept too (it is in any event binding upon me) that the purpose is as described in **Vidal-Hall**. I cannot, however, construe either the Directive or the Act as requiring a data controller to be responsible even without fault for the subsequent disclosure by a third party of some of the information given to it. This is because although the directive has as its principal purpose the safe-guarding of the rights of data subjects, the recitals do not suggest that once a person holds information relating to others as a data controller that person is automatically to be liable for any disclosure by a person who is not acting on behalf of the data controller in making it.

58. Recital 25 to the Directive provides that:

> "Whereas the principles of protection must be reflected, on the one hand, in the obligations imposed on persons, public authorities, enterprises, agencies

> or other bodies responsible for processing, in particular regarding data quality, technical security, notification to the supervisory authority, and the circumstances under which processing can be carried out, and, on the other hand, in the right conferred on individuals, the data on whom are the subject of processing to be informed that processing is taking place, to consult the data, to request corrections and even to object to processing in certain circumstances…"

Recital 46 reads:

> "Whereas the protection of rights and freedoms of data subjects with regard to the processing of personal data requires that appropriate technical and organisational measures are taken, both at the time of the design of the processing system and at the time of the processing itself, particularly in order to maintain security and thereby prevent any unauthorised processing; whereas it is incumbent on the Member States to ensure that controllers comply with these measures; whereas these measures must ensure an appropriate level of security, taking into account the state of the art and the costs of their implementation in relation to the risks inherent in the processing and the nature of the data to be protected";

And Recital 55 says:

> "Whereas, if the controller fails to protect the rights of data subjects, national legislation must provide for a judicial remedy; whereas any damage that a person may suffer as a result of unlawful processing must be compensated for by the controller, who may be exempted from liability if he proves that he is not responsible for the damage, in particular in cases where he establishes fault on the part of the data subject or in case of *force majeure*; whereas sanctions must be imposed on any person, whether governed by private or public law, who fails to comply with the national measures taken under this Directive…"

These recitals recognise the differing levels of protection in Member States; the possibility of *force majeure*, as it is termed, causing problems for data security; and the risks inherent in data processing. They do not speak of a need absolutely to prevent unlawful processing (which would have been all too easy to prescribe if it had been intended) but rather to take "appropriate" measures against it.

59. The definition of "controller" in the Articles of the Directive is effectively that adopted by the 1998 Act. A "third party" is defined as (Article 2f)

> "Any natural or legal person public authority, agency or any other body other than the data subject, the controller, the processor and the person who, under the direct authority of the controller or the processor, are authorised to process the data"

60. In Article 6(1), under "General Rules and the Lawfulness of the Processing of Personal Data" are specified 5 data principles corresponding to data protection

principles 1-5 in the 1998 Act, it being provided by Article 6(2) that "it shall be *for the controller* to ensure that paragraph 1 [i.e. Article 6(1)] is complied with" (emphasis added).

61. Article 17, headed "Security of Processing", which relates most directly to the risk of unauthorised disclosure by the actions of someone who is not acting on behalf of the specific authority of the controller, reads:

> "Member States shall provide that the controller must implement appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction or against accidental loss or alteration unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.
>
> Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected."

62. These recitals and provisions demonstrate that the obligation is placed by the Directive upon the "controller", and that absolute liability for a disclosure was not contemplated by the Directive itself. Counsel between them can point to no case in which it has been held that the DPA imposes obligations which result in absolute or strict liability.

63. Such authority as there is also supports an approach which would deny absolute liability. In **Swinney v Chief Constable of Northumbria** (1999) 11 Admin L.R. 811 a claim was brought under the **Data Protection Act 1984** – and for breach of confidence – when a briefcase containing information relating to a murder enquiry was stolen from a police car, even though the car had been locked and the brief case placed under the driver's seat, at a time when the officers concerned were investigating another matter. Jackson J, as he then was, held that the phrase "reasonable care" properly limited the extent of the duty. Though the 1984 Statute was a predecessor of the 1998 Act, and the latter must be construed independently of its 1984 predecessor since the origin of the 1998 Act is in the Directive, Mr Barnes conspicuously did not argue that in "Swinney-type circumstances" a data controller would be liable. He attempted to draw a distinction between actions such as hacking, a Swinney-type loss of data, or unlawful copying of data by an intruder to the premises where it was kept, on the one hand (where, on his submissions, the data controller would not be held liable provided adequate technological and organisational measures had been taken to safeguard against them) and circumstances such as those in the present case on the other, by arguing that in those examples the third party was an outsider. It was different, he submitted, where the person acting unlawfully and without authority was an insider. Ms Proops QC correctly argues that this is an unprincipled distinction. Insofar as an "insider" (such as an employee of the data controller) processes data unlawfully because that is what he has been told by the data controller to do, or where because he is lawfully authorised to do so by the data controller, his actions are not those of a third party at all. They are in law the actions

of the data controller itself. I agree. If there is to be liability for the actions for an "insider" of this type, rather than an "outsider", this liability must in my view rest upon the principles of vicarious liability to which I shall turn later in this judgment.

64. The short answer therefore, to the claim that Morrisons are liable under the **Data Protection Act** for having broken the data protection principles (other than DPP7) is that they did not, as data controller, themselves offend against those principles. The acts said to break those principles were those of a third party, and not their own.

65. Similarly, the assertion that there is direct liability in respect of breach of confidence or misuse of private information also fails: it was not Morrisons that disclosed the information or misused it: it was Skelton, acting without authority and criminally.

66. DPP7, however, raises different issues, to which I now turn.

DPP7

67. The seventh principle does not impose a duty to take "reasonable care" as such. Those words do not appear in the Statute. This might suggest that the draftsman was aiming at a rather different target when he required that "appropriate" measures be taken. This word comes from the Directive: it is likely therefore to bear an autonomous meaning, which will apply in each Member State of the EU to whom it is addressed. However, it is clear that the principle is a qualified one. The mere fact of disclosure or loss of data is not sufficient for there to be a breach. Rather, "appropriate" sets a minimum standard as to the security which is to be achieved. This is expressly subject to both the state of technological development and the cost of measures. Thus, the fact that a degree of security may technologically be achievable, which has not been implemented, does not of itself amount to failure to reach an appropriate standard: an example might be if particular security measures might be introduced which are very costly at the present stage of development, whereas after a few more years the cost might reduce significantly, as is the case with many new technologies. However, the following words in DPP7 indicate that a balance has to be struck between the significance of the cost of preventative measures and the significance of the harm that might arise if they are not taken. This is itself intended to be a combination of the nature of the harm in itself and the importance of the data to be safeguarded from that harm.

68. Though, as I have pointed out, the words "reasonable care" are not employed, there is a resonance here of the common law approach to the tort of negligence, where the standard of reasonable care is to be judged by balancing the magnitude of the risk of the activity in question (itself a combination of the likelihood of injury and the severity of it should it occur) against the availability and cost of measures to prevent the risk materialising, and the importance of the object to be achieved by performing those actions. That approach is accordingly indicative of the standard which should apply here, whilst remaining mindful that it is being applied in the field of data protection and it is, in general terms, of considerable importance that data be kept secure.

69. Mr Barnes was at pains in closing to remind me that the claim was not a collective one, but rather the claims of several individuals, each of whom uniquely had suffered distress and loss of control over their data. In terms of applying the principle,

however, I have to bear in mind that a breach in respect of any one was likely to give rise not only to the loss or disclosure of that individual's own data, but also of personal information relating to many more. In short, I would expect a higher standard to be observed as to the measures appropriate to protect data relating to 100,000 employees than I would expect in respect of a small enterprise employing 6 or 7 workers. Indeed, with economies of scale, measures that might be prohibitively expensive if analysed per head of a small workforce may seem relatively insignificant if spread over the headcount of a large corporate employer. The magnitude of the risk is greater; the cost per head of guarding against it is less.

Applying DPP7 to the Facts

70. DPP7 stands apart from DPP1, 2, 3 and 5 in that Morrisons were undoubtedly the data controller in respect of the relevant information at the time when the duty fell to be discharged. If appropriate technical and organisational measures were not taken by Morrisons against unauthorised or unlawful processing of personal data then provided that the Claimants could show that that breach of that duty had caused the disclosure which is central to their complaints liability would be made out.

71. The Claimants' case is set out in paragraph 25 of the Particulars of Claim. Mr Barnes submits centrally that it was inappropriate to entrust Mr Skelton with the task of acting as the "middle man" between the sources of information internal to Morrisons required for audit, and KPMG to whom the information was to be submitted. This was not a submission that it was inappropriate to have a trusted human being occupying the role which Skelton did: a matter confirmed by agreed fact 20, that "…it would have been unobjectionable for the Defendant to have used what they refer to as a "trusted employee" to assist with the process of conveying data to KPMG so far as necessary." The reason why Skelton was inappropriate on the Claimants' case was that he had not yet been rehabilitated from very recent disciplinary sanction and was, to the knowledge of the Defendants, unhappy with the way in which the Defendant had dealt with the investigation and disciplinary process. Secondly, the Claimants aver that inadequate steps were taken to ensure that the data, stored for the purpose of copying and onward transmission to KPMG on Skelton's laptop, was deleted from it within a short time after that transfer.

72. Allied to those two central points, the Claimants questioned the manner of transmission of the data to Skelton. It was provided on what was said to be an "…openly readable and transportable USB memory stick as opposed to, for example by secure password protected email." (Particulars of Claim paragraph 25.1.1); there was no adequate management or mentoring of Skelton following the disciplinary process such that he was likely to bear a grudge against the Defendant and his co-workers (25.1.4), Morrisons ought to have discovered that he "subsequently" researched the TOR network on his work laptop; Morrisons failed to supervise, mentor or monitor him so as to prevent his dealing with the information and ultimately disclosing it; and that Morrisons' system should have detected the attempt to send a large file by email from Leighton to Skelton on 14th November 2013. If it had done, "competent investigations would inevitably have identified the obvious risk in exposing the Claimants said information to Mr Skelton" (25.2.2).

73. These contentions became six issues: whether Morrisons fell short of their obligations under DPP7 by:-

a) failing to manage/mentor Skelton "to prevent a grudge developing";

b) failing to monitor the email "quarantine" area so as to identify that the data was being transferred to Skelton;

c) failing to identify that Skelton was researching the "TOR" network;

d) failing to deny Skelton access to the data;

e) providing the data to Skelton via USB stick which it was alleged was not encrypted; and

f) failing to ensure that Skelton deleted the payroll data (in the particulars of claim, the Claimants asserted it ought to have been effective on or about 21st November).

74. There is no other respect in which it is contended that Morrisons fell short of their obligations in respect of DPP7.

The System Generally

75. The payroll data was held on the PeopleSoft system. Any individual had access to their own personal details; managers had access to their own personal details and those of the employees who reported directly to them. No one apart from the approximately 22 "super users" had unfettered access to the data. The existence of any one super user inevitably posed a risk that that person might deliberately or inadvertently disclose data unlawfully. Nonetheless, the Claimants did not criticise this provision, and it is difficult to see how a large commercial organisation such as Morrisons could function without permitting a number of individuals to have access to significant personal data such as that on a payroll file. The case proceeded on the basis that because access was limited, and in any event any use of that access could be tracked (as proved to be the case when Michael Leighton was identified as the individual who had run an SQL query to identify data which was then transmitted to Skelton) the system was appropriately secure.

76. Simon Langley, Chief Information Security Officer told me in evidence that it is impossible for any sizeable data controller completely to exclude the risk that data may be compromised, for example as a result of a criminal hack of its IT systems or the criminal misuse of data by its own employees. In his witness statement (paragraph 14) he said "there is in truth no impregnable system of information security, and even the most intensive state-run security systems are always going to be vulnerable to criminal intrusion or criminal exploitation by insiders as has been shown by data loss at the NSA and intrusions into the systems of the FBI." He saw his role as to assist the data controller (Morrisons) to manage such risks in its operations through the application of appropriate and otherwise proportionate controls. He recognised that the hardest vulnerability to guard against was that of a person with authorised access behaving in a criminal manner.

77. Much of the content of the witness statements of the witnesses called by the Defendant - Daniel Moore, currently "people manager – systems and analytics", who was HR systems manager at the time relevant to the claim; Gordon Graham Daniels,

an internal IT auditor to whom Skelton reported; Jo Goff, Group financial controller who was interim financial controller at the relevant time and who heard Skelton's appeal against his disciplinary sanction; and Alison Charnock, Senior legal officer - expressed their personal views as to the merits of aspects of the claims. Yet no order was made or sought, prior to or at trial, in respect of expert evidence. Insofar as the evidence is of opinion I have therefore disregarded it, save where the fact that a witness was of that opinion is a material fact in understanding or explaining their relevant actions. I have thus relied upon their witness statements for evidence of fact, including those occasions when their view of matters at the relevant time amounts to a fact – for instance, Mr Daniels' view of the reliability of Skelton and Ms Goff's view as to the merits of the appeal. The statement of Lindsey Claire Crossland, director of risk and internal audit was unchallenged, and before me on paper only. She was not appointed to full-time service in Morrisons until after the trial and conviction of Skelton. However, she tells me at paragraph 35 that it would not have occurred to her to subject Mr Skelton to overt or covert monitoring of his IT usage. Nor would she have considered it appropriate. Being unchallenged, I have accepted that evidence.

78. In general, I accept that each of the witnesses did their best to give me an honest and considered account. Mr Daniels was the only witness whose credibility Mr Barnes challenged in closing. I shall deal with that below: in the event, the criticism was more of his reliability of recollection than the credibility of his account.

79. In summary, in any system which permits human access to data there are inevitably risks that that data might be mis-processed, mishandled, or even disclosed without authority. The evidence is that Morrisons took precautions to prevent that so far as they could by limiting access to a few trusted employees only. I am satisfied that the data was protected by restrictions on access, and there were sufficient internal checks available to see which of the few authorised super users had access to the data any more generally than to inquire about their own particulars.

80. The process which led to the disclosure by Skelton involved the transfer to him of data. I accept the evidence of Mr Langley that to extract data from the PeopleSoft database, and store it temporarily on the work laptop of an internal auditor (leave aside, for the moment, the identity of that person) left that data no less secure than it had been while held in PeopleSoft. That is because such a laptop was itself encrypted, and in addition accessible only to one person – he or she who held the encryption key. In setting out the background facts at the start of this judgment, I have already determined that in this case the transfer from Michael Leighton to Skelton was secure: the USB was encrypted, and Mr Leighton took the USB away with him after transfer, which he saw taking place. Moreover, even if the method of transfer had been insecure there is nothing in this case to suggest that that in any way caused the unauthorised disclosure of information contained in the data onto the web in January 2014. I accept that storing the data upon a collator's individual computer, whilst all the data subject to the request from the various sources was collated there, was a sensible system and necessary to provide for an effective audit, enabling the auditors at KPMG to raise queries as to any of the data, and to channel them through one contact. The data so held would, on an encrypted work laptop, be secure. The transfer from a collator of information by downloading it onto a USB stick provided by KPMG and encrypted by them equally gave rise to a risk of data corruption or leak which was merely minimal.

81. As to the deletion thereafter, I accept that data had to remain on the work laptop of the collator for a sufficient period to enable any potential requests for further information from the external auditor to be serviced. Since the work of audit was likely to be completed by early December I would not have considered it unreasonable for that data to have remained on the laptop of the collator concerned until then.

82. It follows that, seen in broad overview, and save for two matters, namely the identity of Skelton himself as the recipient of the information, and the question of whether *in his case* deletion from his computer should have been more carefully checked, there was no failure of Morrisons to provide adequate and appropriate controls. I shall deal with these specific issues below.

Should Morrisons Have Entrusted Skelton with the Data?

83. It is in dispute between the parties whether Morrisons knew or ought reasonably have known that Mr Skelton posed a real risk to the security of the payroll data transmitted to him.

84. Mr Daniels interviewed Mr Skelton before he took up his post with Morrisons in the beginning of November 2010. He thought him able, competent and suitable for the post of a senior IT internal auditor, used to dealing with the complexity of infrastructure and systems of a large corporate organisation. It is probable that Mr Skelton was interviewed also by Mr Chowdhery. He underwent psychometric testing. The results were unexceptionable. Mr Daniels found nothing to make him doubt the trustworthiness of Skelton. He was generally quiet and private. In short, his appointment to the post of Senior IT Auditor, with all the handling of personal data and confidential information that might involve, was entirely appropriate.

85. As to his work, he would regularly be assigned audits which he had to undertake on his own. He was expected to operate with a significant degree of autonomy. His handling of the payroll data central to this case must also be seen in context: apart from that data he regularly had to handle information which colloquially would be termed sensitive or confidential. In doing so, he never gave Morrisons cause before 2014 to doubt his trustworthiness.

86. As to the white powder incident, Mr Daniels recalled Skelton being somewhat frustrated, a frustration he displayed as annoyance but "nothing greater", and that he had been irritated by the level of sanction he received. Skelton did not think that legally posting a legal substance should have resulted in a formal sanction. After that incident he did not display signs to Mr Daniels of being "overly aggrieved" but got on with his job. There was however a change in his apparent motivation. As Mr Daniels put it: "he was a bit up and down and lacked drive and enthusiasm".

87. In summary, in his witness statement, Mr Daniels told me that he thought Mr Skelton had been upset by what had happened but not to the point where he could not be trusted to do the job. His performance had become a bit lacklustre, and Mr Daniels plainly thought he might move on to a company other than Morrisons, but he was still doing good work. Mr Daniels saw what had happened as being a minor incident, in respect of which Mr Skelton had received an appropriate sanction: he viewed the formal verbal warning as a "rap across the knuckles".

88. Although the Claimants criticised the choice of Skelton as the recipient of the payroll data for transmission to KPMG, no questions were asked of the witnesses as to the identity of those who might have been alternative choices. Ultimately though, the question for me is whether it was a breach of DPP7 to allocate the work to Skelton. I assume in doing so that the other one or two internal IT auditors who reported to Mr Daniels appeared competent and trustworthy (since if they did not they would have been excluded from the work) but no more so than Skelton appeared to be, at least before the white powder incident. It is therefore only if there is something about the events which gave rise to the disciplinary proceedings or to Skelton's apparent reaction to them which casts doubt on either his competence or trustworthiness that it can be said that Morrison should have chosen another to be part of the chain of transfer to KPMG.

89. Mr Barnes relies heavily upon a finding at the disciplinary hearing that Mr Skelton had breached the mail room policy and failed to live up to "Morrisons' values". He submits that the censure was not trivial: it led to formal sanction and the report leading to the discipline suggested that Skelton's actions and behaviour viewed on their own could amount to gross misconduct irrespective of the nature of the white powder. By failing to live up to "Morrisons' Values", Mr Barnes said that Morrisons had stigmatised Skelton's behaviour as irreconcilable with the manner in which the Defendant wished to conduct its business. He said this showed that he had failed to live up to the expectations of trust, integrity, teamwork, consideration for others, the sharing of joint objectives and such like stated in the fuller exposition of those Values in the Employee Handbook. The 6 month period during which the warning remained effective indicated that a minimum period of rehabilitation was recognised as necessary. The fact that Skelton appealed showed he lacked insight into his wrongdoing: rather than accept the sanction he chose to challenge the Defendant. Nothing, or nothing much, was done to address his plain disenchantment afterwards. The decision to entrust him with payroll data could not reflect an appropriate approach to the security of that data.

90. In my view, these submissions overstate the significance of what happened. Disciplinary codes such as those adopted by Morrisons in the present case are familiar territory in employment practices. Though Morrisons was perhaps unusual amongst employers in formalising a first verbal warning by recording it in writing (despite the description "verbal") this level represented the very least level of formal sanction. The fact that an informal warning ranked lower does not mean that this warning was of any great seriousness in the eyes of the employer. There was nothing about the incident itself which suggested that Skelton could not be trusted. Indeed, though Mr Barnes spent some time seeking to establish the "Morrisons value" in play was "One Team" , amplified by the explanation–

> "We work together to reach a common goal. It's about keeping our promises, building trust and respect, and valuing each other's contributions"

Jo Goff, who decided the disciplinary appeal, did not accept so far as she was concerned that trust was involved. Though "One Team" was certainly one of the values, the value she had in mind when rejecting the appeal was that of "Great Shopkeeping", which involved the setting of high standards and taking care of details, and in any event the elements of "One Team" centred on working together. In

essence, her view was that in an isolated incident Skelton did not pay sufficient care and attention to the potential impact of his actions on fellow colleagues.

91. In my view, the reaction of Morrisons to what occurred in the white powder incident and afterwards was appropriate. The incident was a minor one, of thoughtlessness: it did not demonstrate any intent to defraud, nor to prejudice colleagues, nor to have Morrisons pay for postage to which he was not entitled in respect of his private business. Many employees have codes which provide for verbal warnings as to particular aspects of their conduct. It cannot sensibly be suggested that employees so warned cannot then be trusted to do their job or require to be supervised. If supervised (the Claimant's suggestion is "mentored") that would almost inevitably be seen by the employee as demeaning, and would in general give grounds for the employee concerned to claim he had been constructively dismissed. There were no grounds for dismissal. There was no basis for supposing that the incident showed that Skelton could not be trusted. It did show that he was on one occasion thoughtless in not anticipating what might happen if those in the post room realised that there was an unknown white powder being sent through their facilities, but no more. I think it was appropriate to regard it, as Mr Daniels did, as a rap across the knuckles.

92. To restrict Skelton's handling confidential data as a result would have been to take an action for which there was, at the time, no obvious logical basis, and if applied consistently would have had to extend to restricting his dealings with other confidential information which it was necessary for him to handle in the course of his employment. He was not just and only concerned with transmitting the payroll data. In effect, as Ms Proops submits, if Morrisons had taken the approach suggested by the Claimants it is difficult to see how he could have done his job. Yet what he did in no way merited dismissal. The sanction imposed fell far short of that. Morrisons could not properly treat it as tantamount in effect to dismissal in Skelton's case.

93. I accept that there was nothing in his lack of motivation to suggest that he had decided criminally to disclose data entrusted to him, harming both his colleagues, to whom the data principally related, and Morrisons, his employer. If Morrisons were to restrict Skelton's access to confidential information upon the basis of the white powder incident their approach in doing so required to be replicated for others who might be human links in a data transmission chain. If a thoughtless action on one occasion could give rise a real risk, which could be prevented only by disallowing an individual, who otherwise had not displayed thoughtlessness, access to data, a similar approach would have to be taken in respect of any employee handling data who might have been transiently thoughtless of others: this would include superusers, auditors, senior managers and so forth. It is not difficult to see that the degree of enquiry to find out if employees had behaved in this way would be intrusive. To institute enquiries of such a nature would be disproportionate to the risk posed. When considering whether Morrisons were in breach of DPP7 on the basis of the white powder incident the balance falls decisively on the "appropriate" side of the line.

94. The evidence showed that the transfer of data from PeopleSoft to KPMG relied critically upon trust being placed in individuals. There was no failsafe system. But the Claimants do not suggest that there should have been. (For instance, I do not know if a double key system, analogous to that used for security deposit boxes in bank vaults, could have been introduced under which data could be accessed on a work laptop only if separate codes were input by each of two individuals who separately

held their own codes and whether if so it would have been viable or would have minimised the risk: it was never suggested and never explored in evidence, and I therefore discount it.) Ultimately therefore the question as to permitting Skelton access to the data comes down to whether it was inappropriate to trust him. The only reason not to do so was the white powder incident, taken together with the hints of disenchantment with work which followed. For the reasons I have given however, the incident itself did not suggest that Skelton was not to be trusted. A lack of motivation does not equate to a positive criminal desire to harm the employer. Taking the two together, the balance still falls on the appropriate side of the line. In short, in permitting Skelton to have the data Morrisons were not in breach of DPP7.

95. Since the incident, procedures have changed a little. Had the revised procedures now utilised been in operation in 2013, it would not have been necessary for an internal auditor who was not a superuser to have handled the relevant payroll data. However, the system as revised still critically depends upon the trustworthiness of human agency. DPP7 is directed towards systems. The risk of human default remains, despite the understandable concerns of Morrisons to guard against it as best they can. The technological and organisational measures current in 2013 and 2014 at their best could not altogether prevent the risk posed by a rogue employee who was trusted and had given no real reason to doubt his trustworthiness.

Monitoring and Mentoring

96. Save in respect of deletion of the data, I can deal with the other control issues shortly. No-one in employment at Morrisons knew, nor ought they have known, that Skelton bore a grudge against the Defendant, and was not to be trusted with data. Suggestion that he should have been managed and mentored within the "rehabilitation period" of 6 months is unrealistic, and mischaracterises the 6 month life of the warning as a "rehabilitation period", as though the employee would have to prove himself within that time. The purpose of expiry after 6 months of a warning is simply that when considering any issue of conduct later arising the employer would not be expected after 6 months to take into account the circumstances giving rise to the former warning. The fact that within the 6 months they might do so acts as a disincentive to an employee to engage again in such conduct, and that represents the control mechanism inherent in a standard disciplinary policy. Beyond saying to Mr Skelton that his conduct in posting a package containing white powder was not acceptable, and explaining why that was (a matter which on the evidence, I find Mr Daniels thought Skelton appreciated, even if Skelton thought it did not merit the reaction of Morrisons to it) it is difficult to see what Morrisons could be expected to do. The "rap across the knuckles" administered was, viewed sensibly, all that was required.

E-mail Quarantine

97. The email sent by Leighton to Skelton, attaching the payroll data, "bounced back" and was held in what could be called quarantine. If the system had been interrogated by a senior manager, it could have been seen that this had happened. If it had been, then the Claimants suggested that this should have alerted the Defendants to the risk which Skelton posed to the data. This is unrealistic. The "bounce-back" involved no action by Skelton himself. There is nothing about it which would indicate that Skelton was any more or less a risk than the risk implicit in the original decision (which I have found not to be inappropriate) to use Skelton as a human conduit in transmission of

data from PeopleSoft to KPMG. In truth, all it would have revealed to any observer was that Leighton had attempted to send too large a quantity of data by email to Skelton. That carries no implications for the subsequent security of the data, especially in a case where, as here, there were encrypted USB sticks available to transfer the data by another means.

Accessing the TOR Network

98. It was suggested in the claim that the Defendant should have been aware that Skelton was attempting to research the TOR network.

99. Mr Langley described that Morrisons have an external facing firewall which is connected directly to the internet. This is known as the "red side". A second firewall protects Morrisons' internal network (the "green" side). Between the two is what is known as a "demilitarised zone" or "DMZ", which can be accessed from the internet but which has very limited access to Morrisons' internal systems, which are protected by the second firewall. An intrusion detection system detects patterns of activity which might indicate a potential attack from the red side. Morrisons also operate a Bluecoat server which is a proprietary web filtering proxy. This both reduces the volume of external internet traffic by storing commonly accessed web pages, so that when two or more members of staff request the same web page only one copy needs to be obtained, and also restricts the sites which staff may access. It captures all requests for internet sites made by someone logged on to the internal Morrisons network, and at the same time maintains a list of restricted websites by reference to categories (e.g. pornographic material). If a request is made for access to a restricted site, the system effectively blocks that access.

100. Morrisons maintain a huge list of restricted sites and update this regularly. One restricted category is "proxy avoidance". This concerns access to those sites which enable individuals to by-pass the restrictions imposed by Bluecoat by accessing the internet by a website proxy. The TOR network is one such proxy avoidance site, and is listed on Bluecoat as such. Accordingly, Mr Langley did not believe it would have been possible for Skelton to access the TOR website itself from which to download software needed to run the TOR network from his work laptop. Even if he were able to do so by some other means Mr Langley's evidence was that he would not have had sufficient administrator access rights to enable him to install that software on his laptop. That would have needed an administrator only password. Only an authorised IT administrator (which Skelton was not) could (and can) install such software on a work laptop.

101. This evidence was not challenged in cross-examination. I accept it.

102. As to whether Morrisons ought to have detected that he had researched or attempted to research the TOR network using Morrisons systems, there was no system enabling Morrisons automatically to detect when employees might be using the system to research the TOR. Nor do Morrisons have such a system in place today.

103. The Bluecoat server keeps a record of every website request made by the end user. Thus, if an authorised person wishes to know what an individual employee has attempted to look at on the internet at work, it is technically possible to get Bluecoat to provide a list. This is not done routinely, but only ever if there is an issue with a

particular employee such that the business feels it to be necessary and appropriate to review that employee's internet usage. Nor would it be common practice in organisations similar to Morrisons routinely to scrutinise employees' web access requests: Mr Langley said he had never in his career come across an organisation which carried out on-going active monitoring of internet searches in order to flag up search material which might be regarded as suspect. In any event, it would be necessary to identify what term was to be subject of the search. To search for such as "TOR" is hopelessly unspecific, for the sequence of 3 letters constituting the acronym appears in a vast number of entirely innocuous longer words – examples were given in his witness statement by Mr Langley of such as "history" or "factory" but it is easily possible to think of many more, particularly since it often forms the last 3 letters of a noun – such as "navigator", "actor", "factor".

104. I find that: -

i) active monitoring of internet searches by employees is not conducted at Morrisons; and this is consistent with the practice adopted by other large companies;

ii) it would be impracticable to do this on a routine basis, in particular because it would involve searching against individuals' usage by reference to a number of terms, and in respect of "TOR" could have produced a plethora of results which would be entirely innocuous;

iii) even if the research had identified that Skelton had searched for information about the TOR network, it would not in itself indicate his unsuitability to be a recipient of payroll data for onward transmission: rather, as an internal IT auditor it might be thought to be a legitimate part of his role, or merely curiosity;

iv) with 3,500 employees based at Hillmore House as was Skelton the resources which would have to be expended to conduct routine active monitoring of the type I have described would simply be disproportionate, if indeed practicable at all (which I conclude it would not have been);

v) in any event, for practical purposes any such arrangement was unnecessary since the firewalls between them blocked undesirable material, and access to dubious websites was considerably restricted by an automatic filter in any event;

vi) Finally, most companies – and I was told Morrisons was no exception – permit employees to access the internet for personal reasons, within reason, and provided this does not conflict with their duties.

105. Moreover, routine monitoring would almost undoubtedly be seen as invasive, and would require a justification on an individual basis before it could properly be conducted. Indeed, in **Barbulescu v Romania** (application 61496/08) [2017] ECHR 754, 5th September 2017) the Grand Chamber of the European Court of Human Rights considered the compatibility of intrusive surveillance conducted by an employer on the electronic communications of an employee. Over 8 days in July 2007 the employer in that case recorded an employee's Yahoo messenger communications in

real time, and on 13th July summoned him to explain the extent of his usage. When the employee said that the usage was for work purposes he was shown a transcript of 45 pages of the messages which he had exchanged with his brother and his fiancée during the period of monitoring. They were all personal, and some were intimate. When he told the employer in writing that he thought the employer had criminally breached the secrecy of his correspondence his contract of employment was terminated. The domestic courts upheld the dismissal.

106. The Grand Chamber decided that they had failed to determine whether the applicant had received prior notice from his employer of the possibility that his communications on Yahoo messenger might be monitored, had paid no regard to the fact that he had not been informed of the nature or extent of that monitoring or of the degree of intrusion into his private life and correspondence. Nor were there specific reasons justifying the introduction of the monitoring measures. The domestic courts should have considered whether the employer could have used measures which intruded less into the employee's private life and correspondence. Accordingly, no fair balance had been struck between article 8 of the Convention, which requires a state to pay respect to private and family life, and the aims and methods of the employer. This case is thus high authority supporting a view that any attempt to institute surveillance of the intensity suggested by the Claimants in the present case would be fraught with the risk of being held unlawful.

107. In the present case, Morrisons had alerted employees through the Morrisons Employee Handbook that it monitored the use of all systems and equipment:

> "to ensure our business is conducted appropriately, including:-
>
> - to establish facts where the content of the communication is disputed
> - to investigate and detect usage in breach of our policies
> - for training purposes
> - for preventing and detecting crime
> - to ensure the effective operation of our systems
> - we will not read all your correspondence, however if an anomaly of concern is found we will investigate this thoroughly."

Nonetheless, to introduce the type of monitoring which could have detected the precise nature of websites being accessed would be a step beyond the sort of supervision indicated by that handbook.

108. Accordingly, even if the implementation of a system that could proactively have detected that Skelton was researching the TOR network when he did was, contrary to my findings, feasible, sensible and practicable, and even if, contrary to my findings, the effort and expense involved in doing it would have been proportionate, it is likely if introduced to have been difficult to justify since it would most probably amount to an unlawful interference with employees' rights to privacy and family life, with little by way of balancing factor to suggest otherwise.

109. Finally, the particulars of claim refer to Skelton's attempt to access the TOR network as having occurred subsequent to his involvement with the data transfer. Since I am of the view that he most probably copied the payroll data to his personal USB on 18th November 2013, it is unlikely that detecting that he had done so at a later stage could have prevented the disclosure of that in 2014. It might perhaps have deterred him from effecting the disclosure, but I consider it more realistic to think that given the careful planning that Skelton had devoted himself to even prior to receiving the data (demonstrated by his searching for TOR on 9th. October, and purchasing a phone for later use, coupled with copying data on to his personal USB on 18th. November, and his devious conduct in using his skills in IT to throw blame onto another), I conclude that on balance, if there had, contrary to my findings, have been a failure to monitor employees' internet search usage it is unlikely that it would have prevented the data disclosure which occurred.

The USB Stick

110. I have already concluded that the USB stick used to convey the payroll data to Skelton was encrypted. Irrespective of whether or not it was encrypted, once the information it contained was copied to his computer it was inevitably accessible by him (just as would have been the case had it come by secure email): he could not otherwise have transferred it from his computer to KPMG. There was no breach of DPP7 in using this means, nor did the use of it cause or contribute to the disclosure which later occurred. It caused no relevant harm.

111. Though there was much cross-examination about Morrisons' policies in respect of data transfer (broadly, disallowing the general use of USB sticks) this was beside the point when considering this specific case. If there was a breach of those policies, it did not constitute a relevant breach of DPP7; but in any event I find the use of the USB in this case was not in breach, since it was specifically understood that for Michael Leighton's purposes in transmitting a large quantity of data internally from one secure site to another an encrypted USB stick would be available for him to use, and he could permissibly use it.

Data Deletion

112. It is probable that Skelton deleted the data a short while after transfer to KPMG, and did so at the conclusion of what would have been a reasonable period of time in which to anticipate requests for further information generated by the audit process KPMG were undertaking (say, until mid-December). Since it is probable that the payroll data was copied to Skelton's personal USB stick on 18th November 2013, and it is to be inferred that this was with a view to the later commission of the crime consisting of disclosure of the data, he would have had no reason to retain the data for longer in any event. It is likely he did delete the data, if only to give the appearance to anyone who looked that it had been removed.

113. I do not consider that Mr Daniels, or any member of Morrisons management, could properly be criticised for not asking Skelton before mid December that the data had been deleted, or checking that it had been. This is because it would have been appreciated that there was a need to keep a copy of the information on Skelton's work laptop and, indeed, as I have already accepted, this was preferable to the alternative (of dipping in and out of the Peoplesoft system) because that would have involved

some risk, albeit small, in the additional transmission of data which that would have necessitated. It therefore follows, too, that there was no breach of the data protection principle of DPP7 if there were indeed a failure to ask or check prior to mid December 2013. Accordingly, since the data had by then probably already been copied the request for evidence of deletion, whether made or not after that time, would have been ineffective to prevent Skelton's subsequent criminal misuse of the data.

114. I consider it likely that Skelton did delete the payroll data from his work laptop. It is known that at some time he removed the data leaving just the template into which that data had been inserted: in March 2014 he showed that empty template (albeit with the headings still complete) to Daniels when he then checked.

115. As to whether Daniels checked prior to that the evidence is mixed. In his witness statement Daniels said:

> "60. It would not have been necessary for Mr Skelton to retain the payroll data for long after it had been passed to KPMG. He might retain it for a relatively short while in case any queries arose, for example, completeness of the data. After that, I would have expected him to delete it, and in his capacity as an IT internal auditor, he would know professionally that it should be deleted. Senior auditors are expected to manage data responsibly.
>
> 61. In fact, I recall discussing with Mr Skelton the retention of the file structure and headings and the deletion of the contents and, later on, asked if he had deleted it and he confirmed to me that he had. My best recollection is that I asked Mr Skelton if the data had been deleted relatively shortly after it had been provided to KPMG because in the normal course and working closely with Mr Skelton that is a conversation he and I would naturally have. I would normally ask this where any sensitive data has been provided to my team and not merely payroll data. I would not have asked to see Mr Skelton's computer to verify this fact, although later on (I do not recall when) I did see the headings that had been left after the data had been deleted from the spreadsheet. I would not, though, usually ask whether a member of my team had deleted data because I would trust them to do it."

116. This passage is muddled. It appears to suggest that he actually remembered having a conversation, then goes on to say only that it is one which he "would naturally have had". It ends with the statement that he would not usually ask whether a member of his team had deleted data, having just said that asking Mr Skelton was a conversation that he would naturally have had. When taxed with this in the course of his evidence, it became clear to me that he had no actual memory of having spoken to Skelton prior to the news of the disclosure of data coming to light. I find that he was struggling to recollect what he actually did, and that his usual practice was not so entrenched as a matter of course that I can be satisfied that he did in fact ask before March 2014. Indeed, as the last sentence of paragraph 61 of his witness statement suggests he did

not generally see the need to ask since he operated on trust. He did have a recollection of seeing the file structure and headings with the data deleted: this, in my view, was most probably around the time that enquiries were being made as to the source of the data leak which had occurred – hence my conclusion that it was most probably March 2014.

117. It follows from this that I find there was no organised system for the deletion of data such as the payroll data stored for a brief while on Skelton's computer. There was no failsafe system in respect of it. To this extent, in my view, Morrisons fell short of the requirements of DPP7: where data is held outside the usual secure repository used for it (in the case of the payroll data, within the Peoplesoft system) there is an unnecessary risk of proliferation and of inadvertent disclosure (let alone deliberate action by an employee) revealing some of that data. Morrisons took this risk, and did not need to do so. Organisational measures which would have been neither too difficult nor too onerous to implement could have been adopted to minimise it.

118. I had the strong sense that within Morrisons' head office systems as they operated in 2013 it would have been regarded as indicating a lack of trust in an employee if a manager were specifically to check that he had performed a process such as deletion. It is right that such checking could in some circumstances be capable of justifying an employee in thinking that his employer lacked the trust in him which was requisite for their employment relationship to continue. However, this does not apply where there is a clear understanding amongst employees, created by management, that it is expected of their managers that they will check to see that files have been deleted, at least where the information they may contain is of sufficient sensitivity. If a culture is developed in which employees expect that as a matter of routine managers will check to see that there has been deletion of data, which has been held outside its usual secure repository, by those with whom it has for the time being been deposited, no employee could be justified in thinking that checking the deletion displayed any lack of trust: it would merely be the employer instituting, maintaining and operating safe and proper systems of checking as normal.

119. I note Mr Langley's view that it was neither realistic nor proportionate to impose an obligation to the effect that managers had to oversee directly and immediately the deletion of data by senior trusted employees, all the more so where the employees' role essentially consisted of the routine processing of significant quantities of sensitive data. However, I do not agree that it would be onerous to institute a system of checking, to be expected within a changed culture such as I have described.

120. I do accept, however, that the risk which primarily would be mitigated by such a system would be that of inadvertent retention of information, and that this on its own could not have prevented an individual determined to do so from copying sensitive data held on his work laptop to some other medium. In the particular circumstances of this case, by the time it would have been appropriate to conduct any such check on deletion, the probability is that the information had already been copied. Thus, notwithstanding that I consider Morrisons in this respect to have failed to discharge their duty to take appropriate organisational measures to guard against unlawful disclosure and/or data loss, to the extent that Morrisons fell short of DPP7 in this respect, this failure neither caused nor contributed to the disclosure which occurred.

Burden of Proof

121. Morrisons maintain that it is for the Claimant to prove breach of any of the Data Protection Principles which they suggest may have been broken, and that the event in respect of which they claim was caused by that breach. The Claimants maintain that the burden is on the Defendant to prove that its arrangements were appropriate. Interesting though this debate is, it is not necessary for me to resolve it in this case. I have had sufficient evidence, to find relevant facts, and to draw conclusions as to the probabilities. I have not had to depend upon the burden of proof. I have not had to resolve any of the issues by reference to it, but rather I have been able to make positive findings in all material respects.

The Inadequate Controls Claim: Conclusions

122. In summary, for the reasons I have given I find that Morrisons did not know nor ought they reasonably to have known that Skelton posed a threat to the employee database; that, save in one respect, there were no control mechanisms which the Defendant ought to have applied in respect of Skelton which were not appropriately applied; that one respect was in relation to the deletion of data but in that case, if appropriate measures had been applied, any reasonable measure that might have been implemented of which I had any evidence or submission would not have prevented Skelton's criminal misuse of the employee data.

Primary Liability at Common Law and Equity

123. Morrisons did not directly misuse any information personal to the data subjects. Nor did they authorise its misuse, nor permit it by any carelessness on their part. If Morrisons are liable it must be vicariously or not at all.

124. It was not in contention that of the elements necessary for a breach of confidence action to succeed, there was information given to Morrisons, and that it was confidential. It was disclosed. However, it was not disclosed by Morrisons either directly or by an agent. In such circumstances, no primary liability attaches to Morrisons for this disclosure. It was a criminal act which was not Morrisons' doing, which was not facilitated by Morrisons, nor authorised by it. It was contrary to what Morrisons would have wished. If Morrisons are liable it must be vicariously or not at all.

125. It follows that there is no primary liability resting on Morrisons under any of the DPA, the common law of misuse of private information, or an equitable action for breach of confidence. There remains the question whether Morrisons are liable as a secondary party for any of the wrongs of which Skelton himself was undoubtedly guilty.

Vicarious Liability

126. Auld LJ in **Majrowski v Guy's and St Thomas' NHS Trust** [2005] EWCA Civ 251, [2005] QB 848 said (at paragraphs 28-29):

> "…vicarious liability is legal responsibility imposed on an employer, although he is himself free from blame for a tort committed by his employee in the course of his employment. Fleming, in The Law of Torts 9th ed. (1998), pp 409-410, observed that this formula represents:
>
> > "A compromise between two conflicting policies: on one hand, the social interest in furnishing an innocent tort victim with recourse against a financially responsible defendant; on the other, a hesitation to foist any undue burden on a business enterprise".
>
> Second, it has traditionally been regarded as taking two forms: first liability for an authorised or negligently permitted unlawful act of an employee in the course of employment; and, second, liability for an employee's unauthorised or not negligently permitted unlawful mode of doing an authorised act in the course of employment. Only the latter is truly vicarious liability; the former is primary liability."

127. Although his judgment was appealed to the House of Lords (where it was affirmed) those passages do not appear to have been contentious.

128. I am concerned here with that which Auld LJ called "truly vicarious liability". The liability is one in which one party without personal fault is held responsible in law for wrongs committed by another. The most common relationship between the person at fault, and the person who, though not at fault is also to be held liable in law in addition to the party at fault, is that of employment, as it is here.

129. The origins of vicarious liability may be unclear: perhaps lying in the rapid growth in the number of employees, and sizes of workforce of enterprises during and after the industrial revolution, and perhaps lying originally in an extension of agency principles. It is unnecessary to say more since the possibilities and history are comprehensively set out in the judgment of Lord Toulson JSC in **Mohamud v William Morrison Supermarkets plc** [2016] UKSC11 at paragraphs 10 – 24.

130. Recent cases have concerned one of two main matters. First is that of the relationships which might render one party to them responsible in law for the wrongs of the other party, since a restriction to those relationships being employment or agency might in some cases be unjust. A notable example is that of **Armes v Nottinghamshire County Council** [2017] UKSC 60 where the judgment of the Supreme Court as to whether a Council might be liable for wrongs done by a foster-parent to whom it had entrusted the care of a child was reported during the closing stages of the hearing before me. This is not, however, a case in which there can be any doubt that the relationship between Morrisons and Skelton was such that vicarious liability might apply. By the end of the 19th century, it had been recognised that an employer might be liable for a wrongful act done by a servant in the course of his employment. The second main consideration in recent caselaw has been the proper approach to "the course of employment". Given that Skelton was an employee of Morrisons at the material time, it is this to which I now turn.

131. The precise scope of "course of employment" which could bring secondary liability upon an employer for a wrongful act was defined by Salmond in the first (1907) edition of his text book on the law of torts, *Salmond on Torts*, as "either (a) a wrongful act authorised by the master or (b) an unauthorised mode of doing some act authorised by the master" adding that a master was liable for acts which he had not authorised if they were "so connected with the acts which he has authorised that they may rightly be regarded as modes – although improper modes – of doing them" (pp 83-84). As Lord Toulson noted in **Mohamud** (paragraph 26) there might be difficulties in the application of this formula in cases of injury to persons or property caused by an employee's deliberate act of misconduct. In **Bazley v Curry** (1999) 174 DLR (4th) 45, in considering the question whether, and to what extent, an employer might be liable for an employee's criminal conduct, contrary to the desires and policies of the employer, MacLachlan CJ saw liability as arising out of twin principles, first that it was just that an enterprise which created risk by its operations should pay if those risks materialised ("enterprise risk"), and second that it was a matter of policy to encourage the employer to exercise the power of control inherent in and essential to a contract of employment so as to minimise any potential harm so arising ("deterrence"). These principles were better served by taking a broad approach to the scope and meaning in this context of "course of employment", and were a significant factor in persuading the House of Lords in **Lister v Hesley Hall Ltd** [2002] A.C. 215, HL that the test of "sufficiently close connection with the employment" should take those two policy considerations into account, effecting a "compromise between two conflicting policies: on the one hand the social interest in furnishing an innocent tort victim with recourse against a financially responsible defendant; on the other a hesitation to foist any undue burden on a business enterprise."

132. There are differences of policy emphasis in the speeches in **Lister**. Lord Clyde's approach (paragraphs 37-42) was to gauge the sufficiency of the connection by asking whether the wrongful acts, in a broad sense, should be regarded as within the sphere or scope of the employment so as to be ways of carrying out the work authorised by the employer; Lord Millett's approach was broader still. He regarded vicarious liability as a species of strict liability, best understood as a "loss distribution device." This echoed the policy concept that he who has the deeper pockets should suffer the impact of a loss where it might fall on more than one party. Lord Hobhouse of Woodborough however focussed on the notion of delegation or entrustment, namely that an employer was vicariously liable for the wrongful act of its employee where it had "entrusted" a duty to an employee who, by his wrongful act, had failed to perform it.

133. **Lister** represented something of a watershed moment in the recent development of vicarious liability so far as concerns liability for the criminal actions of employees contrary to the wishes of their employer. Lord Toulson recognised in **Mohamud** (at para. 40) that the concept of "enterprise risk" has been prominent in cases since **Lister** as the social underpinning of the doctrine of vicarious liability, but added:

> "…the court is not required in each case to conduct a retrospective assessment of the degree to which the employee would have been considered to present a risk. As Immanuel Kant wrote: "out of the crooked timber of humanity, no straight

> thing was ever made." The risk of an employee abusing his position is one of life's unavoidable facts."
>
> "In **Dubai Aluminium Co. Ltd. v Salaam** [2003] 2AC 366, Lord Nichols of Birkenhead (with whom Lords Slynn and Hutton agreed) said (at paragraph 22) "…it is a fact of life, and therefore to be expected by those who carry on businesses, that sometimes their agents may exceed the bounds of their authority or even defy express instructions. It is fair to allocate risk of losses thus arising to the businesses rather than leave those wronged with a sole remedy, of doubtful value, against the individual employee who committed the wrong. To this end, the law has given the concept of "ordinary course of employment" an extended scope.
>
> 23. If, then, authority is not the touchstone, what is?... Perhaps the best general answer is that the wrongful conduct must be so closely connected with acts … the employee was authorised to do that, for the purpose of the liability of the firm or the employer of third parties, the wrongful conduct *may fairly and properly* be regarded as done by the partner while acting in the ordinary course of the firm's business or the employee's employment… (original emphasis)
>
> ……..
>
> 25. This "close connection" test focuses attention in the right direction. But it affords no guidance on the type or degree of connection which would normally be regarded as sufficiently close to prompt the legal conclusion that the risk of the wrongful act occurring, and any loss flowing from the wrongful act, should fall on the firm or employer rather than the third party who was wronged…
>
> 26. This lack of precision is inevitable given the infinite range of circumstances where the issue arises. The crucial feature or features, either producing or negating vicarious liability, vary widely from one case or type of case to the next. Essentially the court makes an evaluative judgment in each case, having regard to all the circumstances and, importantly, having regard also to the assistance provided by previous court decisions."

134. Lord Toulson's judgment continues with an observation that the test of "close connection" might tell nothing about the nature of that connection, but that in **Lister** the court had been mindful of a risk of over-concentrating on a particular form of terminology, and there was a risk in attempting to over refine or lay down a list of criteria for determining what precisely amounted to a sufficiently close connection to make it just for the employer to be held vicariously liable. He said "simplification of the essence is more desirable". As to that he said, under the heading "The Present Law", as follows:-

> "44. In the simplest terms, the court has to consider all matters. The first question is what functions or "field of activities" have been entrusted by the employer to the employee, or, in everyday language, what was the nature of his job. As has been emphasised in several cases, this question must be addressed broadly…"
>
> 45… Secondly, the court must decide whether there was sufficient connection between the position in which he was employed and his wrongful conduct to make it right for the employer to be held liable under the principle of social justice which goes back to Holt CJ. To try to measure the closeness of connection, as it were, on a scale of 1 – 10, would be a forlorn exercise and, what is more, it would miss the point. The cases in which the necessary connection has been found for Holt CJ's principle to be applied are cases in which the employee used or misused the position entrusted to him in a way which injured the third party. **Lloyd v Grace Smith and Co.** [1912] AC716, **Pettersson v Royal Oak Hotel Ltd** [1948] NZLR 136 and **Lister v Hesley Hall Ltd** were all cases in which the employee misused his position in a way which injured the claimant, and that is the reason why it was just that the employer who selected him and put him in that position should be held responsible. By contrast, in **Warren v Henlys Ltd** [1948] 2 All ER 935 any misbehaviour by the petrol pump attendant, qua petrol pump attendant, was past history by the time that he assaulted the claimant…"

135. **Mohamud** was a case in which the Claimant, having stopped at a petrol station at one of Morrisons Supermarkets, went into the sales kiosk and asked the Defendant's employee serving there if it would be possible to print off some documents which the Claimant had stored on a USB stick. The employee refused the request in an offensive manner, and in the exchange of words which followed he used racist, abusive and violent language towards the Claimant and ordered him to leave. He then followed the Claimant as he walked back to his car and, having told him never to return, subjected him to a serious physical attack. In an action by the Claimant for damages against Morrisons on the grounds that it was vicariously liable for the assault the judge at first instance found that the employee had indeed assaulted the Claimant, but dismissed the claim against Morrisons since the employee's actions had been purely for reasons of his own and beyond the scope of his employment such that there was an insufficiently close connection between the two. The Court of Appeal dismissed the appeal. The Supreme Court allowed it. Applying the principles which he had set out (summarised above) Lord Toulson regarded the employee's job as being to attend to customers and to respond to their enquiries, such that the offensive way in which he answered the Claimant's request and ordered him to leave, though inexcusable, was within the field of activities assigned to him, and what happened afterwards was an unbroken sequence of events. Although what he did was a gross abuse of his position, it was in connection with the business in which he was employed to serve customers, a position which his employers had entrusted to him, making it just that as between them and the Claimant they should be held responsible

for the employee's abuse of it. He thought the employee's motive was irrelevant: "it looks obvious that he was motivated by personal racism rather than a desire to benefit his employer's business, but that is neither here nor there."

136. The other members of the court all agreed with Lord Toulson JSC; Lord Dyson added a short judgment of his own emphasising that the second limb of the **Salmond** test was not effective for determining the circumstances in which it was just to hold an employer vicariously liable for committing an act not authorised by the employer. A close connection test remedied the shortcoming and incorporated the concept of justice into the close connection test. He thought however, that it was difficult to see how that test might be further refined.

137. I adopt the approach as set out in **Mohamud**. Since that case was decided the approach has been applied on a number of occasions. I was referred in particular to **Bellman v Northampton Recruitment Ltd** [2016] EWHC 3104, QB; [2017] ICR 543. After a Christmas Party organised by the Defendant about half of those who had been present adjourned to a local hotel, where they sat talking in the hotel lobby, consuming more alcohol. Early in the morning of the next day conversation turned to work. The managing director, who was in overall charge of the company, became annoyed by the discussion and at about 3am assaulted the Claimant employee. The Claimant sought damages against the Defendant company for the actions of its employee, the manager. His claim was dismissed because the judge concluded that, in applying the two stage test, while consideration of the time and place in which the relevant act occurred would always be relevant there had to be some greater connection than the mere opportunity to commit the act offered by the chance of place and time; the assault had been committed after, and not during, an organised work social event; there was not only a temporal but a substantive difference between the Christmas party and the discussion over drinks at the hotel; and the fact that the discussion had turned to work did not turn what was a recreational activity into something which was to be viewed as the course of employment such that there would be a sufficient connection to make it right to hold the company liable.

138. In **Various Claimants v Barclays Bank plc** [2017] EWHC 1929 (QB) 126 the Claimants sought damages against Barclays Bank in respect of sexual assaults to which they alleged they were subjected by a doctor examining them for the purposes of employment by the Bank.

139. Each claimant was required to attend the home of a doctor engaged by the Bank, where he had a consulting room. It was said that in the course of his examination on behalf of the bank he sexually assaulted them. Of the two stage test applicable when considering if the wrongful acts of the doctor had been committed in the course of his employment by the Bank, the principal thrust of the judgment was concerned whether the doctor had a sufficient relationship with the bank for it to be liable for his wrongdoing. Nicola Davies J held that he was an employee. As to the second stage – close connection - she held what he did to be sufficiently closely connected with his employment:

> "46. The alleged sexual assault occurred during the course of a medical examination which the defendant required the claimants to undergo in respect of present and future employment. The task of carrying out the medical examination

> was entrusted to Dr. Bates by the defendant. The task assigned to Dr. Bates put him in a position to deal with the claimants. On the alleged facts he abused that position. It is difficult to see how it can sensibly be argued that his acts did not fall within the activity tasked to him… on the facts I find that alleged sexual abuse was inextricably interwoven with the carrying out by the doctor of his duties pursuant to his engagement by the bank. In the circumstances I find the tort is so closely connected with that employment or engagement to satisfy the second stage. "

Two Preliminary Points on Vicarious Liability

140. Before turning to the application of these common law principles, as set out in **Mohamud** and illustrated by the decisions in **Bellman** and **VC v Barclays Bank** there are two preliminary matters with which I have to deal, raised by Ms Proops QC. The first is whether the **Data Protection Act** by its terms excludes any possibility of vicarious liability. Her argument centres on DPP7. She submits first that the DPA does not recognise any form of vicarious liability for the unauthorised acts of employees, and DPP7 confirms this. Second, she submits that the DPA is such that only data controllers are subject to civil obligations and consequent liability under the Act: neither attaches to any person processing data qua employee or agent of the data controller. In her opening written case, she argued that there was accordingly no statutory civil liability which attaches to a person processing data qua employee and accordingly no civil liability for which a data controller can be held vicariously liable.

141. In my view, this submission in her opening misunderstands the nature of vicarious liability. A party may be held liable vicariously even for a breach of a Statute for which that party could not itself be held liable. Thus where, under the statutory provisions relating to shot firing in mines a duty was placed on the shot firer (but not upon the mine owner or manager), the mine owner or manager might nonetheless be held liable even though neither it nor he could have committed the tort in question. Lord McDermott in **Harrison v National Coal Board** [1951] AC 639, at 671 dealt with the point in a passage which, while strictly obiter, was fully considered.

> "[Counsel for the Coal Board] advanced a further alternative argument to the effect that, the duty in question having been placed on Spence [the shot firer] exclusively, the Respondents could not be made responsible for his breach thereof even if the doctrine of common employment did not apply. In other words, the maxim respondeat superior had no applicability in the case of a statutory duty so laid on a servant. My Lords on the views already expressed it is not strictly necessary to deal with this submission. but it was debated at sufficient length at the Bar to lead me to think that to reserve it for consideration at some future occasion might give it more encouragement than it deserves. It comes to saying that (apart, of course, from the doctrine of common employment) a master is not vicariously liable in respect of his servant's statutory negligence. To my

> mind this, as a general proposition, finds no support in principle or authority. Vicarious liability is not confined to common law negligence. It arises from the servant's tortious acts in the scope of his employment and there can now be no doubt that Spence in breaking the shot firing regulations committed a tort."

142. This approach was clearly endorsed in **Majrowski** in the speech of Lord Nichols of Birkenhead paragraphs 10 – 17. In summary, at paragraph 17 he concluded: "unless the Statute expressly or impliedly indicates otherwise, the principle of vicarious liability is applicable where an employee commits a breach of his statutory obligations sounding in damages while acting in the course of his employment." In the same case, Lord Hope (paragraph 42) noted that Counsel for the employer accepted that he could not succeed in an appeal against the decision of the Court of Appeal below that in general an employer may be vicariously liable for a breach of statutory duty imposed on an employee which is committed in the course of his employment, and that an employer may be vicariously liable for a breach of statutory duty imposed *only* upon the employee. Accordingly, I reject the submission that – if indeed it can be said that direct liability for his acts as data controller in respect of the relevant information was cast by Statute on Skelton alone – this has the consequence that vicarious liability for his breach of the relevant statutory duty was excluded.

143. Further, in **Majrowski** a submission by Counsel for the employer that there was no presumption either in favour or against the proposition that a statute encompassed vicarious liability was rejected: the House held that vicarious liability will apply unless the Statute providing for liability expressly or impliedly indicates otherwise.

144. **Majrowski** itself concerned vicarious liability for an act of harassment (incidentally, necessarily a criminal act under the Statute, since the same acts could either be prosecuted or be the subject of a civil suit) allegedly committed by a co-employee against the Claimant. The Act covered the UK as a whole. In respect of applicability of the Act in Scotland, the Statute expressly referred to the Defender as being the person responsible for the alleged harassment "…or the employer or principal of such person". Had it not been for that provision four of their Lordships expressed the view that the decision would have been finely balanced as to whether the Act, interpreted as a whole but absent that provision, impliedly excluded an employer being held vicariously liable for an act of harassment committed by an employee. Though they expressed some uncertainty one, Lord Nicholls, appeared clear that it would certainly not have excluded this.

145. Central to the judgments was a sense that the **Prevention from Harassment Act 1997**, with which the case of **Majrowski** was concerned, was designed principally to prevent harassment and protect victims from it; and it had an intense focus on the perpetrator in getting him to stop (see per Baroness Hale at paragraph 68). There were "…indeed powerful reasons for thinking that Parliament intended liability and damages should be personal to the perpetrator of the harassment and that it should not be extended to his employer, if any, under the doctrine of vicarious liability…".

146. Undeterred, Ms Proops argues that **Majrowski** has no realm of application in the present case because that decision was not concerned with legislation that plainly does not fix employees (as opposed to data controllers) with any civil liability whatsoever;

the DPA is not concerned with the actions of servants acting in the course of their employment, but rather with the actions of autonomous, self-determining data controllers. The fact that the DPA does not attach liability to a person acting as an employee, as opposed to acting in a distinct, private capacity as an autonomous self-directing data controller, means that there is no statutory wrong committed by the employee on which the principle of vicarious liability could even arguably bite. The scheme is preoccupied exclusively with the direct, not secondary, liability of data controllers. The approach to liability of a data controller under the DPA is fault based, which leaves no room for the implication of no fault vicarious liability on a data controller: she notes that paragraph 10 of Schedule 1 to the DPA provides that the data controller must take reasonable steps to ensure the reliability of any employees who have access to the personal data, not to act as their insurer. Ms Proops submits that under section 13(3) of the DPA a data controller will have a defence if it can show that it took reasonable care to comply with the relevant requirement – in the case of an unreliable employee, that it took reasonable care to ensure that employee's reliability. That provision provides the be all and end all of the responsibility of Morrisons for the defaults of any employee. To permit vicarious liability to run would render that requirement otiose: employers would have little incentive to comply with it if they were nonetheless to be held liable for the actions of their unreliable employees even where they had done their best to ensure that they were reliable. It is a nonsense to suggest that Morrisons, having fulfilled their own obligations qua data controller, can at one and the same time be held vicariously liable for the actions of another third party data controller, who by definition is acting as an autonomous, self-directing controller in respect of the relevant data. There are many good policy reasons why Parliament should have drawn the line as it did. Many, if not most, enterprises would have to process significant quantities of data. It is in the public interest that they should do so. It is very difficult to safeguard the data which such an enterprise processes against employee misuse, as the facts of the present case amply demonstrate. The ease with which employees are legitimately given access to such data gives rise to a risk of copying, extracting or otherwise misusing that data which it is very difficult if not impossible to control. If data controllers are to be held vicariously liable for the actions of their employees, in the absence of any culpable default on their part, that would potentially expose them, unjustly, to enormously burdensome group litigation and claims out of all proportion to the value of the claims of the individual data subjects concerned. Liability on such a scale is disproportionate, yet the legislation itself derives from a European Directive, in respect of the interpretation and application of which proportionality is a key concept. Parliament would have seen that imposing liability for the criminal actions of an individual employee could have a chilling effect on data processing operations across the board. It might introduce a culture of suspicion and indeed paranoia in the work place, for employers might prefer to err on the side of dismissal of disgruntled employees or of subjecting them to draconian invasive surveillance in the hope that that might help to insulate the employer from liability. There is a real risk that the financial viability of some enterprises might be compromised.

147. Before expressing my conclusions on these points, I shall set out the argument on the second point preliminary to considering whether Skelton's actions were sufficiently closely connected to his discharge of the functions assigned to him. This is the submission by Ms Proops that the DPA was intended by Parliament to occupy the entirety of the field of liability for data as defined in the Act, leaving no space within

which any, or any further, actions for misuse of information or breach of confidence could operate. She submits that it is not constitutionally permissible for the courts to enter the field and conclude that Parliament has not gone far enough, or that its legislative work is incomplete, such that further liability should be imposed as common law. Vicarious liability at common law or in equity thus cannot go beyond the liability imposed by Parliament under the DPA which is, in accordance with the first preliminary point (should it be answered in Morrisons' favour), to the effect that liability rests upon Morrisons while acting as data controller alone and excludes liability for an employee separately in breach of his own obligations under that Act. If Ms Proops succeeds on this submission, vicarious liability arises only in respect of the DPA if at all: if it fails, then vicarious liability potentially arises in respect of each and all of the causes of action, subject to the disclosure having been in the course of Skelton's employment by Morrisons.

148. In support of this submission, she referred to **McKerr** [2004] UKHL 12; [2004] 1 WLR 807 in which the question arose whether the courts could impose a common law obligation on the State corresponding to that in Article 2 of the European Convention on Human Rights in an area which had been regulated by legislation. The argument advanced to the House of Lords on behalf of Mr McKerr (whose father had been killed by the use of force by the Royal Ulster Constabulary) was that the Secretary of State was, or should be, subject to a common law obligation to arrange for an effective investigation into his father's death. As to that, Lord Nicholls said at paragraph 32:-

> "The effect of Counsel's submission would be that the court would create an overriding common law obligation on the state, corresponding to article 2 of the Convention, in an area of the law for which Parliament has long legislated. The courts have always been slow to develop law by entering, or re-entering, a field regulated by legislation. Rightly so, because otherwise there would inevitably be the prospect of the common law shaping powers and duties and provisions inconsistent with those prescribed by Parliament….
>
> 33……The suggested new common law right is sought as a means of supplementing, or overriding, the statutory provisions relating to the holding of coroners' inquests. That is not an appropriate role for the common law.
>
> 34. This view is confirmed by another feature of the case. As already emphasised, by enacting the 1998 Act Parliament created domestic law rights corresponding to rights arising under the Convention. When doing so Parliament chose not to give the legislation retroactive effect. In relation to article 2 the intention of Parliament, as interpreted above, was not to create an investigative right in respect of deaths occurring before the Act came into force. The common law right urged on behalf or Mr McKerr would accord ill with this legislative intention. The effect of the propounded right would be to impose positive human rights obligations on the state as a matter of domestic

> law in advance of the date on which a corresponding positive obligation arose under the 1998 Act."

149. Similarly in **Rottman v Commissioner of Police of the Metropolis** [2002] UKHL 20, 2002 2 AC 692, the question before the House of Lords was whether at common law a police officer executing a warrant of arrest issued pursuant to Section 8 of the **Extradition Act 1989** had power to search for and seize any goods or documents which he reasonably believed to be material evidence in relation to the extradition crime in respect of which the warrant was issued. On analysis of the legislation, the House of Lords concluded that there was nothing in it that operated to prevent the continued operation of common law doctrine which had pre-existed the Act. Lord Hoffman said (paragraph 75) "it is a well established principle that a rule of common law is not extinguished by a statute unless the statute makes this clear by express provision or by clear implication." Though the Administrative Court, from which the certified question had come, had held that the **Police and Criminal Evidence Act** ("PACE") had extinguished the common law power to search the Respondent's house five years before the Extradition Act was passed, he could not see any saving provision in it for the common law power. However, the true question was not whether PACE had saved the common law power, but whether it had extinguished or abolished it. Only one provision in the Statute could have had that effect – Section 17(5), which provided that all the rules of common law under which a constable had power to enter premises without a warrant were thereby abolished. As to that, Lord Roger identified the very particular context within which Section 17(5) operated and commented, at paragraph 109:

> "Since Section 17(5) occurs within this very particular context, it is plain that it was intended to abolish only the common law powers relating to entry for the purpose of arrest. The sub-section was not intended to affect the common law relating to searches for evidence carried out when someone has been arrested."

150. Accordingly, since no provision of PACE abolished the common law powers of search and seizure on or after arrest, they continued to operate, and the search with which the House of Lords was concerned was held accordingly to be lawful.

151. In effect, Ms Proops contrasted the position in **Rottman** with that in **McKerr**: in **Rottman** the Act had not had the effect of legislating in the field which common law had previously covered.

152. In **R (Child Poverty Action Group) v Secretary of State for Work and Pensions** [2010] UKSC 54; [2011] 2 AC 15 the question was whether the Department for Work and Pensions could rely on the common law remedy of restitution to reclaim social security benefits paid in error. Section 71 of the **1992 Social Security Administration Ac**t made provision for the Secretary of State to recover overpayments made where there had been misrepresentation or failure to disclose from the person who misrepresented the fact or failed to disclose it. The House agreed that Section 71 was intended to be an exhaustive code. In the speech of Lord Dyson JSC he said:

> "33. If the two remedies cover the precisely the same ground and are inconsistent with each other, then the common law remedy will almost certainly have been excluded by necessary implication. To do otherwise would circumvent the intention of Parliament. A good example of this is ***Marcic***, where a sewerage undertaker was subject to an elaborate scheme of statutory regulation which included an independent regulator with powers of enforcement whose decisions were subject to judicial review. The statutory scheme provided a procedure for making complaints to the regulator. The House of Lords held that a cause of action in nuisance would be inconsistent with the statutory scheme. It would run counter to the intention of Parliament.
>
> 34. The question is not whether there are any differences between the common law remedy and the statutory scheme. There may well be differences. The question is whether the differences are so substantial that they demonstrate that Parliament could not have intended the common law remedy to survive the introduction of the statutory scheme. The court should not be too ready to find that a common law remedy has been displaced by a statutory one, not least because it has always been open to Parliament to make the position clear by stating explicitly whether the Statute is intended to be exhaustive. The mere fact that there are some differences between the common law and the statutory positions is unlikely to be sufficient unless they are substantial. The fact that the House of Lords was divided in *Total Network SL* [2008] AC1174 shows how difficult it may sometimes be to decide on which side of the line a case falls. The question is whether looked at as a whole, a common law remedy would be incompatible with the statutory scheme and therefore could not have been intended to coexist with it."

Conclusions on Preliminary Points on Vicarious Liability

153. As to the first of these two preliminary points as to vicarious liability, the fact that the Act does not provide expressly that there should be vicarious liability is of little assistance to Morrisons: the principle expressed in **Majrowski** is that the principle of vicarious liability is applicable where an employee commits a breach of statutory obligations, even where they rest on him alone, while acting in the course of his employment *unless the Statute expressly or impliedly indicates otherwise.* The House rejected the submission that the principle was neutral.

154. To argue, as Ms Proops does, that the Act imposes liability only on data controllers and that an employee is not a person for whose torts the Act contemplates his employer should be liable vicariously because the employer is not a relevant data controller when the employee processes data in his own right without authority, for his own purposes, and thereby as a data controller, and this is not therefore an "employee's tort" for which the employer can have secondary liability, not only runs contrary to the views expressed in **Harrison v National Coal Board** by Lord

McDermott, but also takes too narrow a view of the Act. The DPA must be seen in its full context: that it is the domestic implementation of a European Directive which describes itself in its title as a Directive "..on the protection of individuals with regard to the processing of personal data and on the free movement of such data." The emphasis is on the protection of data subjects. I accept Mr Barnes's submission that if, at the moment an employee decides to misuse data to which his employer has given him access the employer ceases to be under any further liability, on the basis that the employee thereafter will be data controller in respect of the misuse, this would tend to defeat the rights of data subjects in respect of that data rather than enhance them as is the apparent purpose of the Directive. What, to the contrary, is consistent with the greater security and protection of the data subject is to impose the obligations of data controller upon such an employee (making him liable personally as he would not otherwise be merely qua employee) whilst retaining his employer's vicarious liability for his wrongdoings where it is appropriate to do so. Two parties are then potentially responsible in law.

155. I do not therefore conclude that because the Act has the effect that Skelton became data controller of the information he was later to disclose it, thereby excludes vicarious liability for his breaches of statutory duty under the DPA in respect of that information.

156. A similar point arises in respect of paragraph 10 of Part II of Schedule 1 to the DPA. Ms Proops suggests that by providing that a data controller must take reasonable steps to ensure the reliability of any employees of his the Act indicates that the draftsman intends to restrict the liability of a data controller for the acts of employees, such that an employer is liable only to take reasonable steps to ensure the reliability of an employee, and no further, and that this provision thus implies an exclusion of vicarious liability. Mr. Barnes argues to the contrary: consistent with the overall protective purposes of the Directive, the Act here articulates an explicit protection, which is intended to supplement, not exclude, what would otherwise be liability. In his submission this is strengthened by the fact that in the Directive itself the obligation to take care as to the nature of those to whom data is entrusted is mentioned in that part which relates to the security of data: the liabilities of the data controller are contained in a part of the Directive distinct from this. This, he suggests, shows that the draftsman did not intend the provision to be the sole ground on which an employer could be held liable for an employee, but rather intended to add a specific safeguard for data, which would not depend on there being any infringement by the employer concerned.

157. Ms Proops supports her submission that, upon a proper construction, the DPA impliedly excludes an employer being held liable for the wrongs of an employee of his, by reference to the significant costs of compliance with the data protection principles (see, for instance, **Ittihadieh**, paragraph 26 as to the costs of a single subject access request under the Act). She describes them as giving rise to "enormous and unavoidable up-front costs/burdens for data controllers". To add vicarious liability to this would be to cause already large potential liabilities to be disproportionately crushing in their effect. It would be in addition to "(i) the costs which they incur in physically processing the data (ii) any liability burden to which they may be exposed if they breach their obligations under the DPA" (closing written submissions, paragraph 130(4)), yet Morrisons qua data controller are completely

innocent. It is not, she submits, in the public interest for an "excessive liability" to be visited on an innocent data controller. The possibility of "eye-watering liability" may impose enormous pressure on a data controller to limit the presence of human agency, even where it plays an important role in an effective and efficient operation: to do so is not in the public interest, and the principle of vicarious liability should be designed to serve the public interest.

158. These *in terrorem* arguments are almost certainly overstated: I note that I have not been referred to a single case in which it is said that vicarious liability had overwhelmed a company. I have no doubt this is because many commercial entities will cover the potential losses by appropriate insurance within the ordinary course of trading. Further, since this is by agreement of both Counsel the first case in a period of very nearly 20 years since the Act came into force to raise the question whether there is vicarious liability at all under the Act for the actions of an employee in deliberately misusing the data with which he was entrusted, it seems unlikely that the Doomsday scenarios postulated by Morrisons will occur. This is without yet factoring in both an absence of such cases in respect of the 1984 statutory predecessor of the 1998 Act, and the likely relatively modest award of damages in the event of a finding of liability: I suspect that in many cases the liability may be within the means of an ordinary tortfeasor to satisfy, but, if not, though in a group action affecting a very large number of employees the total sum may certainly be significant, it seems unlikely that the amounts payable would equate, for instance, with those that might be contemplated in respect of a product liability claim asserted by a cohort of injured customers. I accept Mr Barnes' argument on the first preliminary point.

159. There is more to be said for the argument that Parliament has legislated in the field, to leave no space for the common law tort of misuse of private data or the equitable action for breach of confidence. Part of the purpose of the Directive was to achieve a measure of harmonisation of the laws of the member states. It may be thought anomalous, in the field covered by the Directive, that there remain other potential liabilities which depend upon the application of different tests in different jurisdictions. However, it must be remembered that the purpose of the Directive, and therefore the Act, is to provide greater protection for the rights of data subjects. So viewed, additional liabilities in respect of data (insofar as the Data Protection Act creates them, over and above such liabilities as there would otherwise be in equity or at common law) add layers of protection. It is generally open to a member state to augment a minimum EU-wide standard of protection where protection is the aim. Accordingly, thus far, I cannot conclude that the DPA excludes common law and equitable actions in respect of the same data disclosure.

160. As for **McKerr**, the current case is not on all fours with it, for the Court is not being invited to develop the common law by holding that it should move beyond its current boundaries into an area currently regulated by legislation. Rather, the legislation was enacted at a time when the relevant common law duties and obligations were known to exist. In such circumstances, if the common law were intended no longer to operate, the expectation would be that Parliament would say so in terms. The principle Lord Hoffman thought to be well established in paragraph 75 of his speech in **Rottman** is that which is in play: that a rule of common law is not extinguished by a statute unless the statute makes it clear by express provision or by clear implication. There is no express provision here. Nor do I consider that an implication to that effect

is clear. To the extent that the tort of misuse of private information, or an action for breach of confidence can apply in a field also regulated by the DPA is subject to the principles stated by Lord Dyson JSC in **The Child Poverty Action Group** case. The two pre-existing actions do not run counter to the tenor of the Act. Looking at the question as a whole, as Lord Dyson (paragraph 34, last sentence) invites the Court to do I could not hold the common law remedy to be incompatible with the statutory scheme. Both pre-existing forms of action seek to impose liabilities for data misuse or the disclosure of confidential information by both penalising it and making it possible for a court to grant injunctive relief against it. The actions are not so much incompatible as complementary.

161. Accordingly, I reject both the preliminary arguments advanced by Ms Proops QC.

Course of Employment

162. Ms Proops submits that the act central to liability is that of disclosure on the 12th. January 2014. This was not done from work, did not involve a work computer, and was far removed in time from the act of copying the data (which I have already found to have occurred on 18th. November). There was thus such a degree of geographical and temporal separation from Skelton's employment that the act of disclosure could not be said to have arisen in its course. It was even done on a Sunday, when it was common ground Skelton was not at work. Decided cases all showed a much closer connection – in **Rose v Plenty** [1976] 1 WLR 141, CA the employee was on the job, delivering milk; in **Century Insurance Co Ltd v Northern Ireland Road Transport Board** [1942] AC 509 the employee's act of lighting a cigarette by striking a match near flammable fuel came when he was transferring petrol from a delivery lorry to a tank, a job he was tasked to do. Although the cases established that the approach was a broad, evaluative one, such factors as these were of importance. So too was the question whether the act was for the benefit of the employer, although this was no longer a decisive test. Nonetheless, no case had gone quite so far as to hold an employer liable vicariously for an act which, far from being intended to benefit an employer was designed specifically to harm that employer: Lord Clyde in **Lister** at paragraph 44 had recognised, too, when reviewing a couple of cases in which an employee had assaulted another, that acts of passion, resentment or personal spite might fall outside the scope of employment. Here, if the court upheld a plea of vicarious liability by holding Morrisons liable to the co-employees whose personal information had been disclosed by Skelton, the court would be helping Skelton achieve what he criminally set out to do – harm Morrisons financially: it would become a "witting instrument of the criminal".

163. Cases such as **Mattis v Pollock** [2003] EWCA Civ 887 may have involved findings of vicarious liability for assaults which were not committed at the workplace, nor even immediately proximate to it in time of place, but on proper analysis that case was one in which the person for whose acts the employer was held liable was employed specifically to be violent towards customers, as a bouncer, and the act of violence he performed by knifing someone with whom he had earlier been in dispute at the door of his employer's night-club was a logical extension of his employment, tightly connected to his employer's enterprise. **Williams v Hemphill** [1966] UKHL 3 may have been a case in which the driver of a lorry deviated from the route he was supposed to take, but that geographical excursion from the authorised course did not have the consequence that he ceased to be driving on his employer's business – but

even here it was acknowledged by Lord Pearce that this had to kept within sensible limits. To deviate by, for instance, driving from place to place in the home counties via Inverness would on any common-sense view be so well outside his employment as would mean the driver could no longer sensibly be regarded as being in the course of it.

164. Moreover, Ms Proops drew support from the reasoning in **Credit Lyonnais v Export Credits Guarantee Department** [2000] AC 486, in which the House of Lords held that an employer was not vicariously liable for acts of an employee committed in the course of his employment which were not in themselves tortious and only became so when linked to other acts outside the course of his employment. The issue had correctly been identified in the Court of Appeal as:

> "Where A becomes liable to B as a joint tortfeasor with C in the tort of deceit practised by C on B on the basis that A and C have a common design to defraud B and A renders assistance to C pursuant to and in furtherance of the common design, does D, A's employer, become vicariously liable to B, simply because the act of assistance, which is not itself the deceit, is in the course of A's employment with D?"

In the case itself, Mr P (who worked for the Defendant) had been corrupted by bribes from a fraudster, Mr C. He authorised the issue of four guarantees which were an essential part of a fraud which, by the time it occurred, P knew C was committing on the Claimant bank. The issue of the guarantees had in itself no adverse consequences for the Claimant. It was not a tort. Thus P had committed no tort during the course of his employment; what he did, viewed on its own, did not amount to the commission of one.

165. Lord Woolf at 495 C-D said:

> "The conduct for which the servant is responsible must constitute an actionable tort and to make the employer responsible for that tort the conduct necessary to establish the employee's liability must have occurred within the course of the employment. If the tort is committed jointly, then it is conduct which is within the course of the employment sufficient to constitute the tort, irrespective of which tortfeasor performed the acts, which is necessary. As both tortfeasors are responsible for the tortious conduct as a whole in the case of joint torts it is not necessary to distinguish between the actions of the different tortfeasors. For vicarious liability what is critical, as long as one of the joint tortfeasors is an employee, is that the combined conduct of both tortfeasors is sufficient to constitute a tort in the course of the employee's employment.
>
> Were the position otherwise, you could have the extraordinary result that if an employee carried out all the acts complained of there would be no liability on the employer, but if the acts were carried out partly by the employee and partly by a non-employee, the employer would be liable. The obverse situation is the same. If an employer would be liable if the employee personally took the action complained of the situation is no different because some of the acts were done by

> some one who was not an employee as part of a joint enterprise with the employee."

166. What Ms Proops drew from this was a submission that all the acts necessary for the tort complained of had to be committed by the employee in the course of employment. In the present case, the most that could be said would be that some were. That was not enough to make the employer liable on a secondary basis for those acts. Morrisons' submission was that Skelton could not be acting in the course of his employment at a time when Morrisons itself owed no duties to the Claimants in respect of the data: Skelton alone was data controller in respect of that which he disclosed at the time he did so.

167. In an extended review of a number of the decisions which illustrate the way in which principles of vicarious liability have been applied, or a claim for such liability rejected, Ms Proops sought to draw a distinction between actions which pursued a personal, independent venture of the employee by contrast with those in which the employee, though acting contrary to his employer's wishes, and often criminally, was nonetheless within the scope of his employment. The question was raised whether a tort committed against a third party (either a fellow employee or member of the public) whilst the allegedly tortious employee was at work fell on the personal, independent side of the line and not on the side of the "course of employment". It was not difficult to see that if a personal grudge, arising outside the work place, manifested itself in a violent action inside it, where being at work was merely the occasion for an action which might as well have happened elsewhere, it might be expected that the court would hold the employee liable on his own, and that no secondary liability would attach to the employer.

168. In this regard, I was referred to **Deatons v Flew** [1949] 79 CLR 370 (High Court of Australia), and more significantly **Irving v Post Office** [1987] IRLR 289 and **Weddall v Barchester Healthcare** [2010] EWCA Civ 25, all cases in which the Claimants were held to have pursued a grievance of their own, and were held not to be acting in the course of their employment even though (in the first two cases) what they did was at their place of work, and during working hours.

169. In **Deatons v Flew**, a barmaid flung a glass at a troublesome customer, in a moment of retributive rage. In **Irving**, a postman lived next door to the claimant, with whom he fell out. The postman's duties included the sorting of mail at his depot. Just before Christmas, whilst sorting mail, he saw an envelope addressed to the claimant and his wife. Though he did not himself have the duty of delivering the mail to the Irvings, he wrote on the back of the envelope "Go back to Jamaica sambo" (Mr Irving was black). He added a cartoon of a smiling mouth and eyes. When the card was in due course delivered, the Irvings were greatly upset by it. They claimed that there had been an act of discrimination against them contrary to s1(1) of the Race Relations Act 1976, for which the Post Office was (under that Act) vicariously liable. The Court of Appeal (Fox LJ, Sheldon J) applied the dictum of Dixon J in his judgment in the High Court of Australia when it decided that the act of the barmaid in *Deatons* was not an act in the course of her employment:

> "The truth is that it was an act of passion and resentment done neither in furtherance of the master's interests nor under his express and implied authority nor as an incident to or in consequence of anything the barmaid was employed to do. It was a spontaneous act of retributive justice. The occasion for administering it and the form it took may have arisen from the fact that she was a barmaid, but retribution was not within the scope of her employment as a barmaid."

170. As to **Weddall** (on which Ms Proops placed most emphasis: the other two cases were both decided before the decision in **Lister**) the facts were that Weddall was the deputy manager of a care home. A senior health assistant, Marsh, worked under him. They did not get on particularly well. One of the nightshift employees called in sick on a September evening in 2006. In accordance with his duty to secure a replacement, Weddall phoned round to see if an employee could be found to fill the gap. He called Marsh at his home. Marsh was free either to accept or refuse the offer of a voluntary extra shift. He had had a bad day, because of a row at home, and by 6pm was very drunk. He did not react well to the call from Weddall, forming the impression that the latter was mocking him because of his drunken state. Shortly afterwards, he rang the home saying he wished to resign, rode to it on his bicycle, saw Weddall sitting in the garden at the front of the home, and subjected him to an unprovoked, very violent, attack. The first instance judge concluded that Marsh was acting personally for his own reasons, in his own context and on the basis of his own passions and feelings; that an employer was not to be held vicariously liable for every act that one person might commit against another occasioned by or growing from their employment, but not otherwise sufficiently specifically connected with it: it would be neither fair nor just to hold the employer of Marsh (and Weddall) vicariously liable for the acts Marsh had committed. The Court of Appeal had no difficulty in concluding that the judge had reached the right conclusion for the right reasons.

171. Here, Ms Proops submitted that Skelton's act in posting employee data on the web was similar to the act of Weddall. It was a personal action, taken for his own reasons, by way of retribution.

172. In contrast, I was referred to cases which went the other way. In **Bernard v Attorney General of Jamaica** [2004] UKPC 47, a police constable had demanded the use of a telephone from the claimant, who had been in a queue and had just begun to make a call. It was within the scope of the police officer's duty to demand the use of a telephone as a matter of urgency if necessity arose. When the claimant refused, an altercation broke out, ending when the police officer drew a gun and shot the claimant at point blank range, causing him severe injury. A judge in Jamaica upheld a claim against the police force. In turn, the latter's appeal to the Court of Appeal in Jamaica was upheld. However, the Privy Council quashed the Court of Appeal's decision and restored the judgment of the trial judge. It did so by applying the principle in **Lister**, which it plainly considered signalled a change of approach. The police officer had purportedly asserted police authority, immediately before the shooting incident, when seeking priority in the queue for the phone, and it was the fact that the plaintiff was not prepared to yield to this which led to the shooting. Evidence of the constable's later actions in arresting the plaintiff in hospital for interfering with his duties

supported this analysis. Moreover, the State had created the risks inherent in permitting constables to take loaded service revolvers home.

173. The Privy Council reached a further decision to much the same effect in **Brown v Robinson** [2004] UKPC 56, another case of a policeman using firearms in public, when at a football match he was trying to restrain an unruly crowd, when the deceased, Reid, assaulted him and ran off. The policeman then set off in hot pursuit down the road. He asked Reid if he wanted the policeman to shoot him; and, feeling he ought to be taught a lesson did just that and exacted swift retribution for Reid's earlier behaviour. He was seeking to impose a general deterrence and his authority, so that thereafter good order would prevail. It was not a case where there was a private act of revenge unconnected with his employment.

174. In **Fennelly v Connex Southeastern Limited** [2000] EWCA Civ 5568 a ticket inspector assaulted a passenger. The passenger had passed through a ticket barrier where the inspector was checking tickets: as he went on, the inspector called after him "Where is your ticket?" but the claimant walked on further. The inspector followed, and a heated exchange took place. The ticket was snatched from the passenger by the inspector and returned: but immediately afterwards the inspector put the passenger in a headlock and dragged him down a couple of steps or two, that being the assault. A first instance decision on these facts rejecting the claim that there was no vicarious liability, because this act was outside the scope of employment, was reversed on appeal.

175. Mr Barnes also sought to rely on **Axon v Ministry of Defence** [2016] EWHC 787 (QB). The captain of a royal naval frigate was relieved of his command, following allegations against him of bullying behaviour. Three articles were published in the Sun about this, leading to further coverage in the wider media. The Sun disclosed that it had had a source within the Ministry of Defence ('MOD') who had been providing information for some 8 years and who had, over that time, received a total of about £100,000, who had given it the information. She was criminally charged, and sentenced to imprisonment as a result. In an action the Claimant asserted that he had a reasonable expectation of privacy and/or confidentiality in connection with the facts that members of his crew had complained about him, that an Equal Opportunities Investigation (EOI) had been carried out into his conduct, that he had been ordered to leave the Ship whilst it was in Gibraltar and to return to the UK, and as to the outcome of the EOI. Nicol J decided the case against the captain on the basis that he did not have any such reasonable expectation of privacy, but went on to consider the rival arguments whether – if he had found that there was liability – the Ministry would be vicariously liable for the acts of the source.

176. In determining this issue, he took the broad approach to the nature of the job of the primary tortfeasor as advocated in **Mohamud**. The source had worked in a security sensitive environment. She had Developed Vetting clearance which allowed her to have access to information up to the Top Secret classification. With this came obligations. She:

> "..had signed documentation which reminded her of her obligation to maintain confidentiality in information whose disclosure had not been authorised. For someone who occupied such a sensitive position it is in my judgment appropriate to view her job as including the task to preserve that

> confidentiality. ……. she must have learned of that information in the course of her work. I can see no other way that it could have reached her….Of course, for the purpose of examining this issue, I must assume (contrary to my earlier finding) that Ms Jordan-Barber's disclosure to Mr Kay was actionable at the suit of the Claimant. It is only if she committed a tort against him that any issue of vicarious liability could arise. But if that was the case, there is a clear and obvious connection between that wrong and that part of her job which required her to keep such information confidential. If this was the case, then it would seem to me to be just to require the MOD to assume vicarious responsibility. This is not simply an example of the employment being the opportunity for the wrong to be committed. As part of her work, she needed to have access to security sensitive and confidential information. As part of her work she shared office space with the J9 Pol/Ops PJOBS team and was likely to learn other information in consequence. There is always an inherent risk that those entrusted with such information will abuse the trust reposed in them, but rather than this being a reason why vicarious liability should not be imposed, I think, on the contrary, it is a reason in its favour. True it is that Ms Jordan-Barber's activity did nothing to further the MOD's aims, it was carried on without their knowledge, and it received no encouragement from the MOD. What she did was prohibited. However, those features do not preclude vicarious liability (and [counsel for the Ministry] did not suggest they did). Notwithstanding them, if I had held that [the source] had committed a tort (contrary to my findings), I would have concluded that that hypothetical tort would have been sufficiently closely connected with her job for it to be just for the MOD to be vicariously liable."

177. This was the only case to which I was referred in which vicarious liability for a breach of confidentiality/data leak had been considered. Ms Proops submitted that the obiter comments could not be relied on. They rested on a misconceived notion that merely because an employee received or gained access to data in the course of employment this automatically meant that their wrongful disclosure of that data had to be treated as undertaken in the course of their employment irrespective of the actual circumstances. She described this as a "reductionist, decontextualised approach to secondary liability" which was "impermissible in view of the multifactorial analysis which is required in the context of the application of the doctrine of secondary liability".

Discussion

178. In summary, Ms Proops takes seven main points, as well as rejecting the approach taken by Nicol J in **Axon**. First, she submits that the act of posting the data to the web was temporally and physically disengaged from the time when the data was copied by Skelton, and was placed on the web at a time when Skelton was not at work. Second, she submits that at the time he did so, Morrisons were not data controllers within the meaning of the Data Protection Act in respect of the payroll data disclosed. They were not "on the field". Similarly, third, adopting **Credit Lyonnais**, all the aspects of the tort had to be within the course of employment and here they were not. Fourth, the act was motivated by a grudge, and cases such as **Deatons**, **Irving** and **Weddall** showed that this was a significant factor to take into account. Fifth, in **Bernard v Attorney General of Jamaica,** the Privy Council had emphasised that because vicarious liability

is strictly to be applied, it should not easily be extendable: to hold Morrisons liable here would be such an extension, and impermissible. Sixth, to find in favour of Morrisons would amount to the court facilitating a criminal's objective in harming his employer, which the court should set its face against.

179. Seventh, she submits that if the principles articulated by Lord Phillips at paragraph 35 of his judgment in the **Catholic Child Welfare Society** case were considered, they indicated an answer favourable to Morrisons. He said:

> "The relationship that gives rise to vicarious liability is in the vast majority of cases that of employer and employee under a contract of employment. The employer will be vicariously liable when the employee commits a tort in the course of his employment. There is no difficulty in identifying a number of policy reasons that usually make it fair, just and reasonable to impose vicarious liability on the employer when these criteria are satisfied: i) The employer is more likely to have the means to compensate the victim than the employee and can be expected to have insured against that liability; ii) The tort will have been committed as a result of activity being taken by the employee on behalf of the employer; iii) The employee's activity is likely to be part of the business activity of the employer; iv) The employer, by employing the employee to carry on the activity will have created the risk of the tort committed by the employee; v) The employee will, to a greater or lesser degree, have been under the control of the employer."

180. Ms Proops submitted that this was not a case of a single claimant, but of several who together mounted a considerable financial challenge, such that criterion (i) was of little weight – possibly all very well where risks were physical or material in nature, but far more wide-reaching when dealing with data, which was neither; criterion (ii) was inapplicable, since Skelton's activity was not on behalf of his employer but the opposite; as to criterion (iii) Skelton's actions were not part of Morrisons' business activity – Morrisons had left the field; as to (iv) Morrisons did not employ Skelton to carry on that activity, which was not part of his core duties; and criterion (v) was of little weight these days.

181. These points have considerable weight. However, it is rightly agreed between the parties that my task is evaluative, giving such weight to the various factors identified in principle by the courts as the facts of the case require. Illustrative cases do not provide any more than indicative help: interesting as were the cases to which I was referred in respect of grievances, the decision in each was heavily fact-sensitive.

182. Four particular findings of fact are of importance.

183. First, I reject Ms Proops' argument that the disclosure on the web of the payroll data was disconnected by time, place and nature from Skelton's employment. I find, rather, that as Mr Barnes submitted there was an unbroken thread that linked his work to the disclosure: what happened was a seamless and continuous sequence of events. My reasons for this are first that in October, prior to knowing he was again to be a conduit for payroll data between PeopleSoft and KPMG, Skelton showed signs of interest in the TOR network. When he knew (on 1st. November) that he was indeed to be the go-between, he obtained the mobile phone he was later to use just for making the criminal disclosures. He brought in a personal USB stick to work and copied payroll

information to it in mid-November. Lying low for a while after that was necessary to create an appearance of separation and to avoid suspicion falling on him too readily. He again investigated TOR in December; adopted the user name and date of birth of a colleague to draw the blame onto him when setting up an account from which to upload the payroll data to the web; sent data to a web-sharing web-site in January, and either because that did not excite any great immediate interest, or because he had planned in advance to cause the maximum embarrassment to Morrisons immediately prior to the announcement of their financial results, sent the anonymous letters he did to three newspapers in March 2014. These actions were in my view all part of a plan, as the research and careful attempts to hide his tracks indicate. As I have already noted (para. 22 above) this is precisely the same view as that taken by HHJ Thomas QC when sentencing Skelton. This was no sequence of random events, but an unbroken chain beginning even before, but including, the first unlawful act of downloading data from his personal work computer to a personal USB stick.

184. Second, I find that Morrisons deliberately entrusted Skelton with the payroll data. It was not merely something to which work gave him access: dealing with the data was a task specifically assigned to him. Associated with this, I find that in his role with Morrisons, day in and day out, he was in receipt of information which was confidential or to have limited circulation only: and he was appointed on the basis that this would happen, and he could be trusted to deal with it safely. Morrisons took the risk they might be wrong in placing the trust in him.

185. Third, his role in respect of the payroll data was to receive and store it, and to disclose it to a third party. That in essence was his task, so far as the payroll data went: the fact that he chose to disclose it to others than KPMG was not authorised, but it was nonetheless closely related to what he was tasked to do.

186. Fourth, it follows from these findings that when Skelton received the data, though covertly intending to copy it for misuse, he was acting as an employee, and that the chain of events from then until disclosure was unbroken. The fact that the disclosures of 12th. January were made from home, by use of his personal equipment, on a Sunday did not disengage them from his employment.

187. The argument that Morrisons were not "on the field" since they were no longer data controller in respect of such data as was copied by Skelton is misplaced. In part it repeats the argument I have already rejected at paragraphs 153-155 above. The question is not whether Morrisons did wrong, but whether, when Skelton did, his acts were closely connected with his employment.

188. The argument based on **Credit Lyonnais** does not assist Morrisons either. First, it assumes that there was no unbroken sequence of events, but the converse. Second, the issue in that case was very different from the issue here. It was not whether the acts complained of fell within the course of employment but rather whether acts which were committed within the course of employment, which were not in themselves tortious, could be aggregated with acts of another party so as to render the employee a joint tortfeasor with that party, for whose joint acts the employer would be held vicariously liable.

189. As to the act being one of "retributive justice" as Dixon J. would have termed it, arising out of a grudge, it must be remembered that in **Mohamud** Lord Toulson noted

that the motive of the employee was beside the point (paragraph 48). Quite apart from being of the highest authority, this must be right – for the criminal motive of the thieving employee in **Morris v Martin**, or the deliberate dishonesty of the clerk in **Lloyd v Grace Smith** did not convert an act from one in respect of which there would have been vicarious liability into one in respect of which there would not. Earlier in his judgment, too, and consistently with the broad view of course of employment which he espoused, Lord Toulson expressed considerable reservations as to the justice of the result in **Deatons v Flew** (see his paragraph 30). Viewed broadly, the significance of a personal grudge may be, as it were, to bring into the work environment factors which belong elsewhere, so as to make it clear that the only relationship between the tort and work is that the workplace happens to be where it is committed, when it might just as well have been elsewhere. That does not apply here where the grudge was work-related, the central relationship with which it was concerned was that of Skelton with his employer, and its commission was entirely dependent upon the field of activities assigned to him by that employer.

190. Ms Proops' fifth point has limited purchase: though it is true that vicarious liability for the unlawful disclosure of data has only once been considered in any case to which I was referred (that of **Axon**) the principles do not depend centrally on the subject matter of the wrong: it is counter-intuitive to suppose that where the field of activity assigned to an employee concerned anything other than data, that employee would be said to be acting within the course of his employment where, in identical circumstances, save that the field of activity now concerned data, he would not.

191. Ms Proops' sixth line of argument has more traction. Until relatively recently in the history of evolution of vicarious liability the fact that an act was done for the employer's benefit, albeit not as the employer instructed or would have wished, was highly material to a conclusion that the act was within the course of employment. Employment brings with it a duty of loyalty on the servant's part co-relative to the duty of good faith of the master's side. Though benefit is no longer critical, it remains of importance in evaluating whether the relevant tortious act fell within the course of employment. The act here was taken deliberately to harm, rather than benefit, Morrisons. In contractual terms it was a repudiation of the contract of employment.

192. That said, Morrisons were not the only victims. The action here is brought not by Morrisons but by Skelton's fellow employees. They claim not for the harm done to Morrisons, but that aimed at them. Trampling on their rights to the privacy (or confidentiality) of the data was a deliberate act by Skelton. A principal aim may have been to hurt Morrisons, but the method, and it may be an aim as well, was harming their interests. The cases show, too, that the actions of housemasters in abusing children they were employed to care for, of priests in attacking vulnerable victims, of solicitor's clerks in defrauding clients of the firm, or apprentice cleaners in stealing customer's clothing were also repudiatory, and always liable to do serious damage to their employers' business, reputations, livelihood and continued viability, yet in each of these cases vicarious liability has been established. The issue is not so much at whom the conduct was aimed, but rather upon whose shoulders it is just for the loss to fall: the approach since **Bazley v Curry** and **Lister** as developed in **Mohamud** emphasises taking a broad view of the scope of employment, and it is notable that Lord Toulson explained those cases in which liability had been upheld as being those where the employee misused his position in a way which injured the claimant, and

that it was just that the employer who selected him and put him in that position should be held responsible. He was putting great weight on "enterprise risk". I would add to his exposition only that the employer, too, had at least the theoretical right to control. Though employers can hardly tell highly skilled workers the detail of how to do their jobs, it remains a necessary element in every contract of employment that the employer has "…lawful authority to command so far as there is scope for it. and there must always be some room for it, if only in incidental or collateral matters" (**Zuijs v. Wirth Brothers Proprietary, Ltd** (1955) 93 C.L.R. 561, 571, cited by McKenna J. in **Ready-Mixed Concrete v Minister of Pensions and National Insurance** [1968] 2 QB 497): nowadays perhaps best rendered as a directory power. An employer, in general, remains responsible for what work is done, where and when, under what systems and with what equipment, and who the clients or customers are to be. The employer could theoretically place a would-be tortfeasor who is an employee in a position where he could not so easily commit the tort, and design systems to prevent it occurring which the employee could be directed to observe.

193. The factors identified in **Catholic Child Welfare Society** are typically true of relationships of employee and employer, which was what was addressed in paragraph 35 of the judgment of Lord Phillips. They are true here too, where the context is not relationship but course of employment: Morrisons are more likely to have the means to compensate the victim than Skelton and can be expected to have insured against that liability, even if breaches of data security may not historically have been a mainstream risk; it follows from my finding above (ii) that the tort was committed as a result of activity being taken by the employee on behalf of the employer – in the sense of his being chosen to handle the data, with a view to the employer's interests in completing an audit, such that Skelton's employee activity – viewed broadly – can be seen as part of the business activity of the employee, even though he chose to abuse his position. As to (iv), the employer, by employing the employee to carry on the activity, created the risk of the tort committed by the employee; and v) Skelton was, to a greater or lesser degree, under the control of the employer, at least in the sense described in the last paragraph above.

194. Adopting the broad and evaluative approach encouraged by Lord Toulson in **Mohamud,** I have therefore come to the conclusion that there is a sufficient connection between the position in which Skelton was employed and his wrongful conduct, put into the position of handling and disclosing the data as he was by Morrisons (albeit it was meant to be to KPMG alone), to make it right for Morrisons to be held liable "under the principle of social justice which can be traced back to Holt CJ". This conclusion would be the same irrespective of whether a breach of duty under the DPA, a misuse of private information, or a breach of the duty of confidence was concerned, for the essential actions constituting a legal wrong in each case were the same.

195. I am fortified in this conclusion by the views expressed by Nicol J in **Axon**: though insofar as he based his decision upon a view of the source's job as including the task to preserve confidentiality, since she had an obligation to keep matters confidential, I have doubts as to its correctness: where the issue is the identification of the field of activities of an employee, this is not necessarily to be answered by identifying the obligations that are an adjunct to those activities, and are not activities in themselves, which do not in themselves constitute duties specifically entrusted to the employee in

question. Mr Barnes placed some emphasis, in his submissions, on the role of Skelton as being to preserve confidentiality: for the same reason as gives me doubt about this part of Nicol J's judgment, I have placed no weight on this. His role was to handle the payroll data, receiving it, storing it for a while, transferring it to others and then deleting it. All bar the last he did: that is sufficient to draw a close link with his employment, within the principles set out in **Mohamud** and exemplified in case law, and although Morrisons were one target of his actions it is in my view just that they should be liable vicariously for the wrongs Skelton did to the claimants.

Conclusions: Summary

196. In conclusion, I hold that the DPA does not impose primary liability upon Morrisons; that Morrisons have not been proved to be at fault by breaking any of the data protection principles, save in one respect which was not causative of any loss; and that neither primary liability for misuse of private information nor breach of confidentiality can be established.

197. I reject, however, the arguments that the DPA upon a proper interpretation is such that no vicarious liability can be established, and that its terms are such as to exclude vicarious liability even in respect of actions for misuse of private information or breach of confidentiality. Having rejected them, I hold that, applying **Mohamud** principles, secondary (vicarious) liability is established.

198. The point which most troubled me in reaching these conclusions was the submission that the wrongful acts of Skelton were deliberately aimed at the party whom the claimants seek to hold responsible, such that to reach the conclusion I have may seem to render the court an accessory in furthering his criminal aims. I grant leave to Morrisons to appeal my conclusion as to vicarious liability, should they wish to do so, so that a higher court may consider it: but would not, without further persuasion, grant permission to cross-appeal my conclusions as to primary liability.