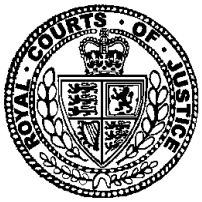

Neutral Citation Number: [2022] EWHC 888 (QB)

Case No: QB-2020-003026

IN THE HIGH COURT OF JUSTICE
QUEEN'S BENCH DIVISION
MEDIA & COMMUNICATIONS LIST

Royal Courts of Justice
Strand, London, WC2A 2LL

Date: 13 April 2022

Before :

THE HONOURABLE MR JUSTICE NICKLIN

- -

Between :

(1) Pamela Underwood
(2) Dominic Underwood
(a child by Pamela Underwood his litigation friend) **Claimants**

- and -

(1) Bounty UK Limited
(2) Hampshire Hospitals NHS Foundation Trust **Defendants**

- -
- -

Max Archer (instructed by **Hugh James Solicitors**) for the **Claimants**
Nicola Atkins (instructed by **DAC Beachcroft Claims Ltd**) for the **Second Defendant**
The First Defendant did not attend and was not represented

Hearing dates: 11-12 January 2022

- -

Approved Judgment

The Honourable Mr Justice Nicklin :

1. This is the judgment following the trial of the Claimants' claims for misuse of private information and alleged breaches of the Data Protection Act 1998 ("the DPA").

A: The Parties

2. The First Claimant is the Second Claimant's mother. She is married to Paul Underwood. The Second Claimant was born, at 02.24 on 16 October 2017, at the Royal Hampshire County Hospital, a hospital within the Second Defendant NHS Trust. The birth was difficult, culminating, after 102 hours, with an emergency caesarean section.

3. The First Defendant ("Bounty") described itself as being a pregnancy and parenting support club. It was based in Welwyn Garden City, Hertfordshire. Bounty provided information and marketed offers and services to parents at different stages of a family's life from pre-conception to pre-school. Bounty's key service was the provision of 'Bounty Packs' (sample packs for different stages of pregnancy and after birth), distributed to new parents. Bounty also provided a mobile application which allowed expectant mothers to track their pregnancies, a new-born portrait service and access to competitions and offers throughout pregnancy and beyond. In addition to this primary function, Bounty also operated a data broking service, providing hosted marketing on behalf of third parties and, until 30 April 2018, it supplied data to third parties for the purpose of electronic direct marketing.

B: Information Commissioner investigation into Bounty

4. The way that Bounty collected and processed data was investigated by the Information Commissioner in 2017-2018. During that investigation, Bounty told the Information Commissioner that it had collected records comprising the following personal data: full name, parents date of birth, email address, postal address, postcode, pregnancy status, status as a first-time mother, name, gender, and date of birth of children (and, by extension, address of child). Bounty informed the Commissioner that during the period 1 June 2017 to 30 April 2018, based upon alleged consent received during the member registration process, it shared a total of 35,027,373 personal data records with Acxiom (a marketing and profiling agency), Equifax (a credit reference agency), Indicia (a marketing agency) and Sky (a telecommunications company) for the purposes of direct electronic marketing. These organisations represented the four largest recipients out of a total of 39 organisations with which Bounty confirmed it shared personal data, with each record shared representing the personal data of an individual person. Whilst the data shared with each organisation varied slightly, in each case it comprised the majority, if not all the data collected in respect of each individual. At the relevant time, Bounty's fair processing notices gave no indication that personal data may be shared with any of these organisations.

5. In response to a subject access request submitted by the First Claimant, the First Defendant confirmed on 23 May 2019 that it held the following data relating to her (and the Second Claimant): her name, date of birth, child's name, child's gender, child's date of birth, home address and email address. The First Defendant also confirmed that it had shared some, or all, of the Claimants' data with 9 third party companies/organisations. Indicia had received all the information, including also details of an IP address and the Master Photographers Association had been provided

with the First Claimant's name, postal and email addresses, due date, baby's date of birth and baby's gender.

6. By a decision dated 9 April 2019, the Information Commissioner held that based upon the information provided by Bounty, any consent to retention and processing of data provided by data subjects was not informed, and the relevant data subjects could not have foreseen that their data would be shared with the third-party organisations. Bounty was found to have shared the personal data of over 14 million individuals to several organisations without informing those individuals that it might do so. As a result, Bounty was found to have processed that personal data unfairly and without satisfying any processing condition under Schedule 2 to the DPA. The Information Commissioner imposed a financial penalty on Bounty of £400,000 pursuant to s.55A DPA for what was held to be a "*serious contravention*" of the first data protection principle in Schedule 1 to the DPA.

C: Events giving rise to the claim

7. Bounty and the Second Defendant had a contractual relationship whereby Bounty was given access to expectant mothers on trust premises. Principally, by a Distribution Agreement, most recently dated 1 June 2016, Bounty agreed to provide Bounty Sample Packs including a Pregnancy Information Folder and Newborn Pack, containing samples, information guides, books, and literature ("the Bounty Pack") for distribution to expectant mothers at the Second Defendant's hospitals. The Distribution Agreement also provided that:

    i) employees of Bounty would attend hospitals to distribute Bounty Packs;

    ii) the Second Defendant would "*use its best endeavours to maximise the distribution of the Pregnancy Information Folders*" and provide daily access to Bounty employees to carry out activities under the agreement;

    iii) Bounty agreed to use information provided "*in strict accordance with the Data Protection Act to mail product information and offers to mothers who express a wish to receive such mailings from Bounty and other reputable companies*"; and

    iv) subject to an upper limit, Bounty would pay 80p to the Second Defendant for each Bounty Pack that was delivered.

8. The Distribution Agreement provided exclusivity to Bounty. The Second Defendant agreed that it would "*not allow competitive services, products, advertising, literature or data collection*".

9. In addition to the Distribution Agreement, the Second Defendant and Bounty also entered a Photography Presentation Service Agreement ("the Photography Agreement"), also most recently dated 1 June 2016. The Photography Agreement provided that:

    i) Bounty would be given daily access to the hospital for the purpose of presenting a photography service at bedsides "*and collecting mothers' name and address information to enable them mother to access the offers presented by Bounty*";

ii) Bounty would provide "*opt-out cards*" for mothers to confirm if they would prefer not to see a Bounty employee;

iii) all data and information would be "*held in strict accordance with the Data Protection Act 1998*";

iv) the Second Defendant would not permit any competitive photography service; and

v) subject to an upper limit, Bounty would pay £1.50 to the Second Defendant for each mother who received a photography presentation.

10. Both the Distribution and Photography Agreements stated that Bounty "*maintains and enforces a strict bedside Code of Conduct regulating Bounty employees' contact and interaction with expectant… mothers*". A copy of a document, headed "*Bounty Code of Conduct – All Bounty Employees*", was included in the trial bundle ("the Code of Conduct"). So far as material, it provided as follows:

> "1. **COURTESY** – Always introduce yourself each day at the maternity ward reception, and ask the ward staff to confirm which mums you can visit – it is imperative that mum has been seen by a midwife after giving birth before you visit.
>
> …
>
> 5. **PRIVACY** – Respect mums' personal space at the bedside, stand far enough away for her not to feel crowded. If the curtains are drawn, NEVER draw them back or peep around the curtain without first informing mum that you are there and asking her if she would prefer to come back later.
>
> …
>
> 7. **DATA PROTECTION** - Always ask mum if she wishes to give permission for her details to be shared with Bounty and other carefully selected companies. (Provision of mums' contact details and permission is NOT a condition for receiving the Bounty bag)
>
> …
>
> 10. **BOUNTY PORTRAIT** – offer mums the opportunity to have a photo taken, take pride in offering the highest quality portrait possible, but NEVER pressure her to accept the offer or purchase at bedside.
>
> **REMEMBER – All Bounty Services are offered on the basis of choice and this code respects mums' freedom of choice.**

11. Following the investigation by the Information Commissioner, it is tolerably clear that, notwithstanding the ability to 'opt out' noted in the Code of Conduct, Bounty's business model was largely based upon harvesting data from expectant mothers in order to sell that data on to third parties. The provision of Bounty Packs was the 'hook', or incentive, to get expectant mothers to sign up and provide personal data which was obviously considered to be commercially valuable by Bounty.

12. The First Claimant had no idea of these commercial arrangements between the Second Defendant and Bounty. Her first connection with Bounty was when, on or around 2 April 2017, she provided her name, address, date of birth and email address to Bounty. She also provided her due date and confirmed that this was her first child. In her evidence, the First Claimant said that she had signed up, using the Bounty App, to receive Bounty Packs. She said that the service had been mentioned by her midwife, but she had also already heard of Bounty online.

13. After a long labour, the First Claimant gave birth to her son following a caesarean section in the early hours of 16 October 2017. She returned to the post-natal ward to recuperate. Her husband was with her. On the ward there were several other beds. Limited privacy was obtained by pulling a curtain around the bed. The First Claimant stated in her evidence that she was physically worn out following the birth, describing herself as being "*in a zombie-like state*". In her evidence, the First Claimant stated that shortly after she had been returned to the ward someone, who she assumed to be part of the maternity staff, came through the curtain that was drawn around her bed and started talking to her and her husband. She said that she was too tired to engage in communication, and so left matters to Paul. She did recall that he was angered by this person "*hovering around the end of [her] bed and looking at paperwork*".

14. In his evidence, Paul Underwood stated that he was aware of Bounty and that his wife had signed up with them prior to the birth of their son. Mr Underwood had been with his wife for the duration of her labour. He confirmed that a woman had arrived at their bedside by walking through the curtain. The person did not introduce herself, and Mr Underwood initially assumed, from her confident manner, that she was a member of the hospital staff. He said that she had arrived at an inconvenient moment when he was cleaning up some blood that had got onto the floor. Mr Underwood described that she had gone straight to the end of the bed "*and started rummaging around in the paperwork holder… located at the end of Pam's bed*". It was only when the person mentioned the opportunity to have photographs taken that Mr Underwood began to be suspicious as to whether she was a member of staff. The First Claimant, he said, asked directly who she was, and she replied that she was a Bounty representative. Mr Underwood described her as being insistent that they should have photographs taken to capture their "*first family portrait*"; it was, he said, a "*sales pitch*". Mr Underwood told her that it was neither the place nor the time for photographs. Both parents remember there being some further mention of child benefit before the Bounty representative left. Mr Underwood estimated that she was with them for some 6-7 minutes before he had insisted that she should leave. In cross-examination, Mr Underwood stated that he had needed to ask her several times before finally she left. The First Claimant, in her evidence, described the Bounty representative as having walked around her bed in a "*blasé like fashion as if she personally knew me and my family*". Following the complaint, the Second Defendant introduced an opt-out scheme that would allow mothers to decline the Bounty services. Subsequently, the Second Defendant terminated its commercial arrangement with Bounty on 19 July 2019 following the ICO investigation and financial penalty imposed on Bounty.

15. Mr Underwood stated in his evidence that he was annoyed and disturbed at this intrusion. He said that he was insistent that she should leave and was not wanted there. He recalled that the woman had used Dominic's name, information he believed she could only have obtained from looking at the notes at the end of his wife's bed.

Subsequently, he raised a complaint with the hospital feeling that the incident had been unacceptable and "*quite frankly disgusting*".

16. After returning home, the First Claimant stated that it was not long before she started to receive targeted emails and telephone calls from several "*random companies*". She and her husband suspected that these had been caused by their interaction with the Bounty representative on 16 October 2017. As it turns out, it is more likely that these communications were the result of the First Claimant's original signing-up to Bounty in April 2017. When she gave evidence at trial, the First Claimant stated that her main complaint was her data being sold on to third parties by Bounty but also that the Second Defendant had allowed the Bounty representative to disturb her following the birth of her son on 16 October 2017. She said that she was furious that someone had come onto the ward, when she was at her most vulnerable, and had obtained information to which they had no right. The First Claimant said that she was in a space that she should have been able to trust, and her data had been obtained. She felt that this was wrong.

17. Documents in the trial bundle, which have been obtained by the Claimants from the First Defendant, include two records showing the data that the First Claimant held about the Claimants. The first of these documents appears to record the data that the First Claimant had provided when she first signed up with Bounty on 2 April 2017 ("the First Data Record"). This information, necessarily, does not contain data about the unborn child (e.g. name and gender) beyond his/her expected due date. A second document records data of both the First and Second Claimants held by Bounty ("the Second Data Record"), which included the Second Claimant's name, gender, and date of birth, although this is incorrectly recorded as 15 October 2017. Interestingly, this Second Data Record incorrectly records the First Claimant's date of birth, whereas the First Data Record (containing the data originally provided by the First Claimant herself) correctly records the information provided.

D: The civil claim

18. Following a letter of claim, dated 11 October 2019, the Claim Form was issued on 27 August 2020. It sought declarations and damages from both Defendants arising from alleged breaches of the Data Protection Act 1998 and misuse of private information. The Particulars of Claim, served with the Claim Form, largely concentrated on the alleged wrongdoing of the First Defendant. The claim against the Second Defendant was more limited and alleged that it had "*allowed the First Defendant to access the ward and the medical records, thus enabling the First Defendant to collect and ultimately distribute the [Claimants'] Private Information*". By reason of these alleged breaches, it was alleged that the Claimants had lost control of their private information resulting in its distribution to an unknown number of third parties. The Claimants included a claim for general, aggravated and exemplary damages. No claim is made against the Second Defendant that it is liable – vicariously or otherwise – for the acts of the Bounty Representative. Nor is it contended that the Second Defendant had, itself, disclosed any personal information relating to the Claimants to the First Defendant.

19. The Second Defendant filed its Defence on 23 October 2020. It accepted that it had a commercial relationship with Bounty (as described above), and pursuant to that had permitted a Bounty representative access to the ward on 16 October 2017, but made no admissions as to what had taken place at the First Claimant's bedside when she was visited by that representative. The Second Defendant contended that much, if not all, of

the private information said to have been wrongfully obtained/misused had been provided by the First Claimant when she had initially signed up to Bounty in April 2017. Any further information that had been provided by the First Claimant on 16 October 2017, for example her son's name, had been provided by her voluntarily. It had not been provided by the Second Defendant.

20. The First Defendant has not participated in the proceedings. The company went into administration on 3 November 2020. Having read the Joint Administrators proposals dated 9 November 2020, it appears that following appointment of the administrators, a sale of part of the business and assets of the First Defendant was completed to Bounty Joy Limited. In terms of the remaining assets of the First Defendant, the administrators estimated that there were insufficient funds to enable a distribution to unsecured creditors. The Claimants obtained judgment in default against the First Defendant on 12 November 2020. I am not aware that any steps have been taken to enforce that judgment against the First Defendant.

21. The Claimants also included in their claim a separate complaint that the Second Defendant had failed to respond adequately to a subject access request made under s.7 Data Protection Act 1998. This claim was not pursued at trial, so I say nothing more about it.

E: The evidence at trial

22. The evidence at trial consisted of the documents in the agreed trial bundle and the witnesses. Three witnesses gave evidence: Mr and Mrs Underwood, for the Claimants and Hilary Goodman for the Second Defendant. At the time of the relevant events, Ms Goodman was the Deputy Head of Midwifery for the Second Defendant.

23. My impression of the witnesses was that each of them was honest and doing his or her best to assist the Court with their recollection of relevant events. Mr and Mrs Underwood still felt strongly about the behaviour of the Bounty representative on 16 October 2017 and more generally they felt that Bounty had exploited the Claimants' personal data. I can certainly understand why they would feel this way. There was a particular section of the witness evidence – concerning what documentation was available at the end of the First Claimant's bed on 16 October 2017 (see further [33]-[36] below) – that appeared to me to demonstrate, first, the value of oral testimony in explaining and resolving apparent areas of dispute and, second, the honesty of the witnesses.

24. In Section C above, I have already set out the evidence of the Claimants, which I accept, describing the relevant events. Insofar as I need to resolve any other factual matters to determine the issues in dispute, then I deal with them below. As I have already noted, the only factual issue of any significance, that I will need to resolve, is the issue of the information/data that it is likely that the Bounty representative accessed when she was seen to look at documents at the end of the First Claimant's bed. I deal with that below.

25. I have not included in this judgment all the evidence that was relied upon by the parties. For the purposes of resolving the dispute, it has not been necessary to do so. For example, some of the evidence (and part of the cross-examination) concentrated on the complaints raised by Mr & Mrs Underwood regarding the behaviour of the Bounty

representative and later about the sharing of the Claimants' personal data by Bounty (and, it was alleged, the Second Defendant).

F: Issues to be resolved

26. The Claimants' claim, as argued at trial, focused on the alleged responsibility of the Second Defendant for disclosure of private information of the Claimants to the Bounty representative on 16 October 2017. It is alleged that the private information that Bounty obtained was the names of the Claimants, their dates of birth, the Second Claimant's sex, the Claimants' postal address, the First Claimant's email address, the First Claimant's status as a first-time mother and IP address. The Claimants accept that, when the First Claimant signed up with Bounty on 2 April 2017, she provided much of this information, but they contend critically not the Second Claimant's name, sex and date of birth. This information, it is alleged, was taken by the Bounty representative from the "*medical records*" or possibly from other documents that were available at the end of the First Claimant's bed on 16 October 2017. The Claimants allege that the Second Defendant took no steps to ensure that the Claimants' personal data was properly protected.

27. There is a substantial overlap – in terms of facts – between the Claimants' case for breach of the Data Protection Act 1998 and the claim for misuse of private information. In respect of the former, the Claimants contend that the Second Defendant "*processed*" the Claimants' data, under s.1(1)(c), by disclosure of the information/data by "*otherwise making available*" the relevant information/data to Bounty. In respect of the latter, the Claimants contend that the obtaining of the information/data by the Bounty representative was a misuse of private information for which the Second Defendant is liable.

28. The Claimants' case is neatly encapsulated in the following paragraph of their skeleton argument for trial:

> "The Trust made the Claimant's Private Information available to Bounty on 16 October 2017. It did so through its arrangements with Bounty whereby its employee was given access to the Claimants. Their information was available to be gathered either by way of the feeding chart and other medical notes in full view, and/or by knowingly allowing the Bounty employee to gather information from Pamela herself when she was exhausted, confused and unfit to make informed decisions about her data".

29. As no claim is made that there was a deliberate act of disclosure of the Claimants' private information by the Second Defendant, the Claimants' claim depends on demonstrating a culpable omission by the Second Defendant.

30. In the light of the above analysis, the issues that require resolution are as follows:

    i) what information/data was contained in the documents that were stored at the end of the First Claimant's bed or thereabouts?

    ii) what (if any) information/data was obtained from these documents by the Bounty representative?

iii) was the obtaining of that information either (a) a breach by the Second Defendant of the Data Protection Act 1998; and/or (b) a misuse of private information by the Second Defendant?

iv) if so, what remedies should the Court grant to the Claimants in respect of the breach(es)/misuse that has been established?

(1) What information/data was contained in the documents that were stored at the end of the First Claimant's bed or thereabouts?

31. This is an issue of fact. The Claimants' case was that the First Claimant's medical records were kept at the end of her bed. This was disputed by the Second Defendant. The evidence of Ms Goodman was that patients' medical records were kept securely in the ward office and could only be accessed by mid-wives and the ward clerk. Bounty representatives were not permitted to access patients' medical records.

32. Ms Goodman's evidence on this point was not substantially challenged in cross-examination. Mr Archer did attempt to suggest to Ms Goodman that she could not rule out that medical records were left by a patient's bedside, but Ms Goodman remained firm in her evidence. She made the point in her evidence that there are strict procedures for protecting medical records which are strictly enforced by the Care Quality Commission. I accept Ms Goodman's evidence. Medical records are well recognised to contain highly sensitive and private information. It is not likely that they would simply have been left – in breach of the procedure outlined by Ms Goodman – by the First Claimant's bedside. The Claimant has not proved that her medical records were available at the end of her bed or thereabouts.

33. However, that finding does not resolve the matter. It was plain from the First Claimant's evidence that there were some documents at the end of her bed and, indeed, that she had looked at them. She specifically recalled that the form she had looked at had a space where her new son's head measurements were to be inserted. This information was missing from the form when she had looked at it. She had recalled that, particularly, as it was information that she was curious about. There was some suggestion that the document could have been a feeding chart that may have had Dominic's name and date of birth on it. The First Claimant had remembered filling out the feeding chart. Ms Atkins suggested to the First Claimant that it was likely that it was the feeding chart that the Bounty representative had looked at. The First Claimant, understandably, did not know whether that was right. When re-examined, the First Claimant was asked whether she could recall any other information that was on this form. She answered that it had his weight and the time, date and mode of birth.

34. When Ms Goodman gave evidence, she reiterated that medical records were kept in the ward office not at the bedside, but she confirmed that a new mother would have a feeding chart in her bed area which she would be encouraged to complete. Ms Goodman stated that the feeding chart would show the mother's name, hospital number, address, and the child's date of birth, but no other information. Ms Goodman was also able to shed more light on the document that the First Claimant had described when she gave evidence. Immediately following birth, the newborn baby is visited by a paediatrician who carries out an examination and records various observations on a new infant physical examination form ("the NIPE form"). Ms Goodman confirmed that frequently the NIPE form would be partially completed by a midwife and then left in the bed area

so that it could be completed by the paediatrician following the examination of the child. Ms Goodman, who had heard the First Claimant give her evidence during the trial, thought that the document that she had described was the incomplete NIPE form. Dominic's head circumference, which the First Claimant had noted was not recorded on the form that she had seen, would have been one of the data inserted after the paediatrician's examination.

35. I have no difficulty in accepting this evidence and explanation by Ms Goodman. As I have noted above, it is a good example of loose ends of evidence being resolved during the trial process. The First Claimant had clearly recalled something memorable about the form she had seen – the absent data about the measurement of her new son's head. Based on this, Ms Goodman was able to identify, from its description and the practice on the maternity ward, that it was a NIPE form which had not yet been completed fully.

36. I am therefore satisfied on the evidence that it is likely that the incomplete NIPE form had been placed at the end of the First Claimant's bed and was one of the documents that could have been seen by the Bounty representative when she looked at the documents as described in the evidence of both Mr and Mrs Underwood. The partially completed data would have included the Second Claimant's name, his gender (whether expressly or by implication from the name) and his date of birth. It is likely that the feeding record, that would also have contained Dominic's name and date of birth, was also available.

(2) What (if any) information/data was obtained from these documents by the Bounty representative

37. Again, this is a matter of fact. The only evidence that bears on the question of whether the Bounty representative did see one or both documents, and obtain data from it/them, is the Second Data Record (see [17] above). On the one hand, this evidence is consistent with the Bounty representative having harvested data relating to the Second Claimant from the NIPE and/or feeding record. However, the error with the Second Claimant's date of birth undermines this and supports, instead, an inference that this data was in fact a deduction made by the Bounty representative from matters she had observed. On the other hand, the Second Data Record does include the Second Claimant's name and both parents were clear that they had not given Dominic's name to the Bounty representative.

38. On balance, my assessment is that the Claimants have proved that it is likely that the Bounty representative saw the feeding chart and/or the incomplete NIPE and, from that, she had obtained Dominic's name (and thereby his gender). The Claimants have not proved that she obtained Dominic's date of birth from those records. Had this information been obtained from the available documents, it is likely that his date of birth would have been accurately recorded by the Bounty representative. The inaccurate recording of the date of birth in the Second Data Record leads me to find that this was a conclusion drawn by the Bounty representative from her meeting with the Underwood family not data obtained from any of the documents that she saw. The balance of the information relied upon by the Claimants, relating to the First Claimant, had been provided by the First Claimant when she originally signed up with Bounty not from the events on 16 October 2017.

(3) Was the obtaining of that information either (a) a breach by the Second Defendant of the Data Protection Act 1998; and/or (b) a misuse of private information by the Second Defendant?

39. This is a mixed question of law and fact. The issue of fact is the circumstances in which the NIPE and/or the feeding record came to be seen by the Bounty representative. The question of law is whether, based on the factual findings, the Second Defendant is liable for the alleged breach of data protection and/or misuse of private information.

40. No one suggests that the Second Defendant directly disclosed information relating to the Claimants to the Bounty representative or that it authorised or encouraged her to consult or obtain data from the NIPE and/or feeding record. On the contrary, I would find, as a fact, that such use the Bounty representative made of those documents was unauthorised by the Second Defendant and should not have happened. Although not expressly forbidden by the Bounty Code of Conduct, its omission was perhaps because it was obvious that representatives should not be looking at patient documents/records.

41. Is the Second Defendant nevertheless liable for the Bounty representative obtaining the Second Claimant's name and gender from these documents? This liability is alleged to arise from a failure to prevent the Bounty representative gaining access to the relevant documents. In my judgment the answer is no.

42. Largely, this result follows from a simple application of the legal test to be applied to the Data Protection Act 1998 and in misuse of private information.

43. In respect of data protection, I reject the submission that, by placing the NIPE and/or feeding record at the end of the First Claimant's bed (or thereabouts), the Second Defendant had disseminated or otherwise made available the relevant data. Mr Archer was unable to find any domestic authority on the point. He relied instead upon ***Mircom International Content Management & Consulting (MICM) Ltd -v- Telnet BVBA*** (C-597/19), a decision of the CJEU of 17 June 2021. The judgment concerned the proper interpretation of "making available to the public" in the Copyright Directive 2001/29/EC. The Court held [47]:

> "In order for there to be an 'act of communication', and consequently, an act of making available, it is sufficient, in the final analysis, that a work is made available to a public in such a way that the persons comprising the public may access it, from wherever and whenever they individually choose, irrespective of whether or not they avail themselves of that opportunity… The concept of an 'act of communication' refers, in that regard, to any transmission of the protected works, irrespective of the technical means or process used".

44. I do not find this authority of assistance to the interpretation of whether data has been made sufficiently available by a data controller to amount to processing of the data for the purposes of the Data Protection Act 1998. On the facts, Mr Archer's argument must be rejected. In no sense could the acts of the Second Defendant, in making available to the Claimant and other members of the Second Defendant's staff documents necessary for the care and treatment of the Claimants, be regarded as making those documents available to the Bounty representative or generally. The simple truth is that the Bounty representative was acting inappropriately (and probably unlawfully) by looking at those documents. If she had asked the Second Defendant's staff if she could read them,

permission would rightly have been refused. The Second Defendant is not liable for the unauthorised (and unlawful) acts of the Bounty representative.

45. Ms Atkins submitted that the Second Defendant had, at all times, processed the Claimants' data lawfully and in accordance with the Data Protection Act 1998. Any access to data by the Bounty representative on 16 October 2017 was unauthorised. It was not processing data authorised by the Second Defendant and in respect of any such processing by Bounty, the Second Defendant is not liable as a data controller: ***Ittihadieh -v- 5-11 Cheyne Gardens RTM Company Ltd*** **[2018] QB 256** [70]-[71]. I accept Ms Atkins' submissions. The Second Defendant has not processed the data of the Claimants in contravention of any part of the Data Protection Act 1998.

46. In substance, the Claimants' claim is for an alleged breach of the Seventh Data Protection Principle; failing to take appropriate technical and organisational measures to prevent unauthorised processing of (or access to) the Claimants' personal data. Mr Archer contends that the Second Defendant had, pursuant to the commercial agreements with Bounty, permitted Bounty representatives to have access to the maternity ward. He argues that the Second Defendant carried out no assessment of the risk of data breach by representatives gaining unauthorised access to patient data. Mr Archer submits that the Second Defendant's staff seem to have "*stood by while the Claimants were harassed by the Bounty employee*". However, Ms Atkins submits that this claim must fail on the evidence. The Claimants' medical records were kept in the ward office. Insofar as personal data was contained in forms that were available at the Claimant's bedside, then inclusion of that limited data was necessary for the Second Defendant and its staff to discharge its duties. The commercial arrangements with Bounty did allow access to the wards, but this access was to be exercised by Bounty representatives in accordance with the Code of Conduct. That Code of Conduct emphasised the need to respect the privacy of each patient and to abide by the requirements of the Data Protection Act 1998.

47. I reject Mr Archer's submissions on this point. The Bounty representative conducted herself in a way that was not in accordance with the spirit or letter of the Code of Conduct. Simply, she should not have been reading the NIPE and/or the feeding record. There is no evidence that members of the Second Defendant's staff "*stood by*" and permitted the Claimants to be harassed or documents to be accessed. Although I shall treat that submission as something of an advocate's flourish, it is both unjustified on the evidence and unwarranted. But more than that, a functioning hospital cannot do its job without making available at least some limited data about patients. Unavoidably, some of that data may come into the hands of third parties. For example, a notice may be placed above a patient's bed warning of an antibiotic intolerance. A nurse administering medication may (as part of a failsafe) ask for a patient's name and date of birth to ensure that the correct medication is being provided, in circumstances where a visitor with a neighbouring patient may overhear that information. Obviously, the hospital authorities would take steps to prevent people collecting and recording this information if such activities came to their attention. But the decision whether a data controller has taken "*appropriate technical and organisational measures… against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data*" (Seventh Data Protection Principle), is fact sensitive and requires a sensible accommodation of these various rights and interests.

48. I have no hesitation in rejecting the complaint that the Second Defendant has breached the Seventh Data Protection Principle by failing to prevent the Bounty employee from reading the NIPE and/or feeding chart. One only needs to consider the alternative to see why the Claimants' argument must be rejected. To avoid liability on this ground, all patient data would have to be strictly withheld. Presumably, a new mother would have to ask to be provided with the feeding chart, complete it, and then have it collected back and returned to secure storage. It seems to me to follow from Mr Archer's submission that plain words on a notice warning of a patient's antibiotic intolerance would perhaps have to be replaced with some code intelligible only to staff. The inconvenience and risk, were it necessary for such steps to be taken to avoid liability under the Seventh Data Protection Principle, demonstrate that such measures are neither appropriate nor necessary.

49. The claim for breach of the Data Protection Act 1998 must be dismissed.

50. In respect of the claim for misuse of private information, there is no dispute as to the applicable principles of the tort. Liability for misuse of information is determined applying a two-stage test: (1) does the claimant have a reasonable expectation of privacy in the relevant information; and (2) if yes, is that outweighed by countervailing interests: ***McKennitt -v- Ash*** **[2008] QB 73** [11]; ***ZXC -v- Bloomberg*** **[2022] 2 WLR 424** [26]. The contentious issue in this case is whether the Second Defendant is guilty of acts sufficient to amount to misuse/interference under the tort.

51. Mr Archer submits that there has been little consideration of this element of the tort in the authorities, which have tended to concentrate on publication cases. In his argument, he noted that, in ***Various Claimants -v- Wm Morrisons Supermarket plc*** **[2018] EMLR 3113 (QB)** [66], Langstaff J had found that the supermarket had not disclosed the information or misused it, but an employee. More recently, in ***Warren -v- DSG Retail Ltd*** **[2021] EMLR 25**, Saini J followed Langstaff J's decision in ***Morrisons*** and rejected a claim that the defendant was liable for misuse of private information ("MPI") arising from a data breach following computer hacking. In his judgment, the Judge found:

> "[27] I accept that a 'misuse' may include unintentional use, but it still requires a 'use': that is, a positive action. In the language of art.8 ECHR (the basis for the MPI tort), there must be an 'interference' by the defendant, which falls to be justified. I have not overlooked the Claimant's argument that the conduct of DSG was 'tantamount to publication'. Although it was attractively presented, I do not find it persuasive. If a burglar enters my home through an open window (carelessly left open by me) and steals my son's bank statements, it makes little sense to describe this as a 'misuse of private information' by me. Recharacterising my failure to lock the window as "publication" of the statements is wholly artificial. It is an unconvincing attempt to shoehorn the facts of the data breach into the tort of MPI."

52. Although Mr Archer has attempted to distinguish the facts of the Claimants' case from ***Morrisons*** and ***DSG*** (relying principally upon the speech of Lord Nicholls in ***Campbell -v- MGN*** **[2004] 2 AC 457** [15]), in my judgment his argument must be rejected. Based on the facts found, there has simply been no 'misuse' of the Claimants' private information by the Second Defendant. I am wholly unpersuaded that, on what the Second Defendant has done or failed to do in this case, it can be liable under the

MPI tort. The Second Defendant has, itself, provided no information to Bounty about the Claimants. My findings about the limited extent to which Bounty obtained information about the Claimants following the unwanted visit by the representative on 16 October 2017, such data/information was obtained without the Second Defendant's consent or knowledge. It is insufficient to sustain a cause of action in MPI that the Second Defendant *permitted* the Bounty representative to have access to the Claimants. To the extent that there has been an unauthorised obtaining of private information relating to the Claimants by the Bounty representative (which is limited in any event), the Second Defendant is more wronged against than wrongdoer.

53. Although not a point that received any real attention at the trial, even if the Claimants had established that the Second Defendant was liable under the MPI tort for Bounty acquiring information about them, the information so obtained was trivial. Discounting the information that the First Claimant had already provided to Bounty voluntarily when she originally signed up for its products and services, this amounted only to the name, gender and date of birth of the Second Claimant. To be actionable for misuse of personal information, the information misuse must reach a level of seriousness before the tort is engaged. Had the claim not failed for other reasons, it would have failed on this ground.

54. For this reasons, the Claimants' claim in misuse of private information must also be dismissed. I appreciate that this decision will be a disappointment for the Underwood family, but in my judgment the real wrongdoer here was Bounty not the Second Defendant.

55. As a result of my findings, judgment will be entered for the Second Defendant on the Claimants' claim. In consequence, no issue as to remedies arises. However, I should record that the claim for exemplary damages ought never to have been included against the Second Defendant. On behalf of the Claimants, Mr Archer did not press the claim at trial (but neither did he formally withdraw it). Claims for exemplary damages are wholly exceptional. The cases in which such damages can properly be claimed are very few; those in which they are awarded fewer still. It is never appropriate to add a claim for exemplary damages simply to mark how upset the claimant is about the defendant's conduct, or as some sort of negotiating strategy. The Particulars of Claim did not disclose a proper case for an award of exemplary damages against the Second Defendant. Happily, it appears that no significant time or costs has been expended on this issue, but as a matter of principle claims for exemplary damages should only be pleaded where there is a proper basis to do so and supported by admissible evidence or in the expectation that such admissible evidence will be available at trial.