Neutral Citation Number: [2023] EWHC 938 (KB)

Case No: QB-2020-000862

IN THE HIGH COURT OF JUSTICE
KING'S BENCH DIVISION

Royal Courts of Justice
Strand, London, WC2A 2LL

Date: 25/04/2023

Before:

MR JUSTICE CHAMBERLAIN

- -

Between:

ISMA ALI	**Claimant**
– and –	
THE CHIEF CONSTABLE OF BEDFORDSHIRE POLICE	**Defendant**

- -
- -

Jack Scott (instructed by **Irvings Law**) for the **Claimant**
Jennifer Oborne (instructed by **Legal Services Bedfordshire Police**) for the **Defendant**

Hearing dates: 14 February 2023

- -

Approved Judgment

This judgment was handed down remotely at 10.30am on 25 April 2023 by circulation to the parties or their representatives by e-mail and by release to the National Archives.

.....

MR JUSTICE CHAMBERLAIN

Mr Justice Chamberlain:

Introduction

1 On 1 March 2019, the claimant Isma Ali telephoned Bedfordshire Police ("the Police"), for which the defendant is responsible, to pass on information about her ex-husband, who she believed was dealing drugs. She wanted action to be taken against him and said that she believed he posed a risk to her and her children. She also made very clear that she did not want to be identified as the source of the information. She met a police officer, who made a report, which recorded that she was "frightened of repercussions from speaking to the police". The report was passed on to the Social Services Department of Luton Borough Council ("Luton"). An employee of that department who happened to be in a relationship with Ms Ali's ex-husband unlawfully accessed and downloaded a copy of the report and passed it to him.

2 Ms Ali filed a claim against Luton, alleging that it was vicariously liable for the unlawful conduct of its employee. That claim should ideally have been heard with this one, but it was not. It was heard by Richard Spearman QC, sitting as a Deputy High Court Judge, in January 2022 and dismissed on 27 January 2022: see [2022] EWHC 132 (QB). Luton was held not vicariously liable for the unlawful (and indeed criminal) acts of its employee.

3 The present claim is brought on the basis that, although the Police had a duty to pass to Luton Borough Council the information that Ms Ali had given them, they did not need to pass on the fact that Ms Ali was the source of it. Ms Ali contends that, in doing so, they breached her rights under Articles 5 and 6 of Regulation (EU) 2016/679 ("the General Data Protection Regulation or "GDPR"), misused her private information, breached her confidence and acted incompatibly with her right to respect for her private life under Article 8 of the European Convention on Human Rights ("ECHR") and therefore contrary to s. 6 of the Human Rights Act 1998 ("the 1998 Act").

The facts

4 The claimant gave evidence and was cross-examined. The defendant's evidence was given by Police Sergeant Steph Webb, Andrew Taylor and Kevin Sharp. All were cross-examined.

5 On 1 March 2019, Ms Ali telephoned Crimestoppers in a state of distress. She said that her ex-husband had been dealing cocaine, she was scared of him and she did not want him to be around her children. She made clear that she did not want to be identified as the source of the information she was passing on. She did not want a police officer to come to the house because he had installed cameras there. She did not want to go to the police station because he knew people there. She did not want a police officer to come to her parents' house because he knew people in the vicinity. She was concerned that the police might share the recording of the conversation. The call handler, an employee of the Police, told her: "I will make sure that I write all over it that you don't want your name being shared. You haven't even told me your name so I don't even know it."

6 A short time later, after she had checked the Police's databases, the call handler called Ms Ali back. Ms Ali was worried because the call handler now had her name and

number. They agreed that a police officer would meet Ms Ali in a nearby Asda car park. Ms Ali again made clear her concern that she should not be identified.

7 Steph Webb (then a Police Constable, now a Police Sergeant) was in the vicinity with a student officer, PC Norman. They were asked to meet Ms Ali. They were told that Ms Ali had reported domestic incidents involving her ex-partner. PC Webb called Ms Ali, who asked her not to activate her body worn camera when they met. She remembers having to arrange several meeting places. They finally met at the third one. She recalled that Ms Ali refused to get out of her car because she was paranoid about people driving past and recognising her. This level of anxiety made PC Webb concerned. There was at least one child in the back seat behind Ms Ali.

8 While at the roadside, there were points where Ms Ali was upset. PC Webb completed a crime report and a DASH form. (DASH stands for "domestic abuse, stalking and honour-based violence".) The form poses questions. Question 2 was "Are you very frightened?" The answer was "Yes. Frightened of repercussions from speaking to police." Question 3 was "Are you afraid of further injury or violence? If so, please give an indication of what the abuser might do and to whom? (E.g. kill themselves or injure the children)". The answer was "Yes. He has never hit me before, but Im [sic] worried he could. I think he is a violent person." Question 14 was "Is the abuse getting worse?". The answer was "Yes. He has brought drugs into the house near our children. I have heard him talking about dealing and threats to destroy anyone who defies him. I don't know who this is about but it worries me." Question 15 was "Does the abuser try to control everything you do and/or are they excessively jealous? (In terms of relationship, who you see, being 'policed at home', telling you what you wear for example. Consider honour based violence and stalking and specify this behaviour.)" The answer was "Yes. He has access to my CCTV cameras so can monitor whos [sic] at my house. This isn't stalking behaviour but it means I am worried to contact police as he would see they have come to my home and ask me what about."

9 PC Webb completed a child risk assessment which gave a "risk rating" of "medium" and contained the following justification:

> "[The children] reside at Perrymead with their mother, Isma. Badar is the father of both children. Although the children appear well cared for, appear fit and well, look healthy and well nourished, the nature of this report concerns Badar keeping large quantities of cocaine at the address they reside. This exposes them to the risks of coming into contact with this drug and also exposes them to the risk of drug related crime occurring at that address. There is also suspicious [sic] that Badar consumes drugs and may be in an intoxicated state around them, presenting further risk to them. In addition to this, Isma suspects that Badar has access to firearms. This is unconfirmed and there is no believed to be any firearms present at the location, however this presents an obvious risk if true."

10 After filling in the crime report and DASH form, PC Webb had no further involvement with the case. The crime report and DASH form were passed to Andrew Taylor, who worked in the Public Protection Unit ("PPU"), which he described as "the front door to the Police's safeguarding teams". Mr Taylor's role involved processing reports from police officers about members of the public who may be vulnerable. He explains that

any report of a domestic incident where there has been a grading of medium or high risk to children will always be shared with the relevant local authority. On 2 March 2019, Mr Taylor was on duty in the PPU hub and considered the crime report and DASH form relating to Ms Ali. Having read these he concluded that there was more than sufficient information for him to make a safeguarding referral to Luton Borough Council. The safeguarding referral was generated by the Athena computer system and Mr Taylor emailed it to Luton Borough council via their secure network. Mr Taylor's evidence was that the sharing of information in this way was necessary to prevent unnecessary risks to children.

11 Mr Taylor was asked about the process in cross-examination. If a report was made by a neighbour (for example), the name of the reporting party would not be recorded, but where the report came from the victim, the name would always be recorded and the form would never be anonymised. It was always sent to the local authority unaltered. In his view, the risk of inappropriate disclose was met by sending the material by secure email.

12 About 4 weeks after the referral was made, a social worker from Luton came to visit Ms Ali. In late April or May 2019, Ms Ali's family and friends started to ask her questions about her calling the police on her ex-husband. She began to suspect that the information she had provided had been passed on. She started having panic attacks and stayed with her parents for a while before changing her mobile phone number and asking the Council to rehouse her. She came off her social media accounts and tried to hide from her ex-husband. She felt trapped and suicidal. She often cried and found it difficult to concentrate at work. She was prescribed anti-depressant medication and sleeping tablets.

13 Ms Ali later discovered that the reports passed by the Police to Luton had been downloaded and passed to her ex-husband by an employee of Luton, Rhully Begum, with whom he was in a relationship. She pleaded guilty before Luton Crown Court to an offence under s. 1 of the Computer Misuse Act 1990 and on 12 October 2020 was sentenced to 3 months' imprisonment, suspended for 12 months, together with 150 hours of unpaid work.

14 Meanwhile, Ms Ali made a complaint to the Police. It was dismissed on 13 October 2019 on the ground that the duty to safeguard Ms Ali's children from harm meant that they were obliged to pass on not only the information she had given them about her ex-husband but also its source. Ms Ali pursued the matter to the Independent Office for Police Conduct ("IOPC"), which on 27 November 2019 upheld her appeal and directed a reinvestigation. On 16 June 2020, the complaint was rejected by the Police again after a second investigation.

The law

The GDPR

15 Article 5(1) of the GDPR provides as follows:

> "Personal data shall be:
>
> (a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');
>
> (b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');
>
> …
>
> (f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')."

16 Article 6(1) provides:

> "Processing shall be lawful only if and to the extent that at least one of the following applies:
>
> (a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
>
> (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
>
> (c) processing is necessary for compliance with a legal obligation to which the controller is subject;
>
> (d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;
>
> (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
>
> (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

> Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks."

17 The Police entered into an Information Community Agreement ("the Agreement") with various bodies involved in the delivery of services for children and vulnerable adults, including Luton. The Agreement appears to have been drafted in 2015 and to have been reviewed and updated in August 2016. In its current form it notes that sharing information between agencies is lawful in a variety of circumstances, including where "the public interest in sharing the information outweighs the obligation of confidentiality owed to the individual such as safeguarding a child or vulnerable adult's welfare (this would be on a case by case basis and not the sharing of large volumes of data)" (emphasis added).

Misuse of private information

18 Misuse of private information is a tort distinct from breach of confidence. Information is private for the purposes of this tort if the person in question has a reasonable expectation of privacy in respect of it. If so, the question is whether that expectation is outweighed by a countervailing interest: *ZXC v Bloomberg LP* [2022] UKSC 5, [2022] AC 1158, [43]-[62]. In *ZXC,* the countervailing interest was the publisher's right to freedom of expression. However, countervailing interests can be wider than this: see e.g. *Dixon v North Bristol NHS Trust* [2022] EWHC 3127 (QB), [44]. There was no dispute that they could in principle include the need to protect individuals from harm.

Breach of confidence

19 There are three essential elements of breach of confidence: first, that the information was confidential in nature; second, that it was communicated in circumstances importing an obligation of confidence; and third, that there was an unauthorised use of the information: *Coco v AN Clark (Engineers) Ltd* [1968] FSR 415. However, a breach of confidence may be justified in the public interest if there are sufficiently weighty reasons to override the duty of confidence: see e.g. *Toulson and Phipps on Confidentiality* (4th ed., 2020), para. 5-165. Again, there was no dispute that a disclosure that would otherwise be actionable as a breach of confidence could in principle be justified by the need to protect individuals from harm.

Article 8 ECHR

20 It was agreed on all sides that the disclosure by the Police to Luton constituted an interference with Ms Ali's right to respect for her private life within Article 8(1) ECHR. If the disclosure was necessary for the purposes of the GDPR and/or the torts of misuse of private information and breach of confidence, then it was also necessary for the protection of the rights and freedoms of others for the purposes of Article 8(2). If not, the disclosure to Luton was incompatible with Article 8 and therefore contrary to s. 6 of the 1998 Act.

Submissions on liability

21 Jack Scott for the claimant submitted that Ms Ali was clearly assured that her name would not be passed on. To establish that it was lawful for the Police to pass on to Luton the fact that the information about Ms Ali's ex-husband came from her, the

Police would have to show that this was necessary. That is a question for the court. There was no evidence from Luton Borough Council (i) that it was necessary to know that Ms Ali was the source of the information or (ii) that their response would have been slower or different if they had not known the source of the information. In this case, no balancing exercise was undertaken. No-one considered at the time of the referral whether it was necessary to share the source of the information. This means that the Police cannot establish that it was "necessary" to share the fact that she was the source of the information. This in turn means that the Police cannot establish that the disclosure was necessary for the purposes of the GDPR, nor that there was a sufficient countervailing interest for the purposes of misuse of private information, nor a justification for the purposes the law of confidence or Article 8(2) ECHR.

22 Jennifer Oborne for the Police submitted that the claimant had no reasonable expectation that her identity as the source of the information she provided would not be passed to Luton. She relies on an exchange in the first call to Crimestoppers where Ms Ali asked "would you mention me in this at all?" and the call handler replies: "If you are at risk and you need help then we would have to action on it". She submits that the promises of anonymity were made during the first two calls. Even then the focus is on ensuring that the claimant's ex-husband does not find out and nothing there could be taken as an assurance that the claimant's identity as the source of the information would not be passed on to Luton.

23 In any event, Ms Oborne submitted that s. 11(2) of the Children Act 1989 imposes an obligation to make arrangements for ensuring that its functions are discharged having regard to the need to safeguard and promote the welfare of children. That duty includes an obligation to protect the claimant (as the children's mother). Given that the Police had to pass on the fact that the claimant was at risk in order to protect her and her children, it also necessarily had to pass on the fact that she was the source of the information. This is because the identity of the source was necessary to assess the credibility of the information provided and understand the level of risk and because it would not have been possible to redact the information to enable her not to be identified as the source of it. Thus, passing on to Luton the fact that Ms Ali was the source of the information she had given was "necessary" for the purposes of Article 6 GDPR and was justified for the purposes of the law of misuse of private information and breach of confidence.

Conclusion on liability

The claim under the GDPR

24 The transcripts of the two calls between Ms Ali and the call handler establish clearly that Ms Ali was very concerned about any disclosure by the Police that she was the source of the information. She repeatedly asked for assurances that her identity as the source of the information would not be revealed. She was even concerned that the call handler should not say her name aloud in case anyone heard it. No-one reading the transcripts as a whole could be in any doubt that the call handler had assured Ms Ali that she would not be identified as the source of the information, although the Police might nonetheless have to take action based on the information it had received. This is what Ms Ali wanted. I accept Ms Ali's evidence that, if any suggestion had been made

that the Police might pass on to Luton her identity as the source of the information, she would have terminated the call immediately.

25 Whatever was said at the meeting with PC Webb, the circumstances of that meeting could only have confirmed how important it was to Ms Ali that her identity as the source of the information should not be revealed: she refused to leave her car, so a discussion lasting about 30 minutes had to take place through the car window; and the DASH report records her fear of "repercussions from speaking to police". Although there was no specific discussion about disclosure of Ms Ali's identity as the source of the information to Luton, it should have been obvious that Ms Ali had not consented to that.

26 Both sides agree that the Police had to pass on to Luton the information that Ms Ali had given them. The question is whether it was justified in also passing on the fact that the information had come from her. It is clear from the evidence that no-one working for the Police ever considered this issue at the time when the referral to Luton was made. This was not the fault of PC Webb. Her job was simply to fill in the DASH report; it was not for her to consider what to do with it. Mr Taylor did have to consider what to do with it. But his evidence is that it was not part of his function to consider whether it should be anonymised. As he understood it, the only question was whether to pass on to Luton the information in its entirety, including the identity of its source, or not to pass on any of it.

27 The key issue in this case is whether the disclosure by the Police to Luton of Ms Ali's identity as the source of the information was "necessary" for one of the purposes identified in Article 6(1) of the GDPR. Mr Scott is correct to say that Article 6(1)(f) is inapplicable here, but I approach the case on the basis that the Police are entitled to rely on Articles 6(1)(b) and (c), even though neither of those was expressly pleaded in the defence. Such an approach gives rise to no prejudice to the claimant: both sides have come to court to address the question whether the Police's disclosure of Ms Ali's identity as source of the information was necessary to protect her and her children.

28 In the human rights context, the question whether an interference with a Convention right is "necessary" is for the court, giving such weight as is appropriate to the view of the public authority whose decision is under challenge: see e.g. *R (Begum) v Denbigh High School Governors* [2006] UKHL 15, [2007] 1 AC 100. I would apply the same approach to the question whether a disclosure is "necessary" for one of the purposes set out in Article 6 of the GDPR. I do not think that anything said by Nicklin J in *Dixon* suggests the contrary. The submission he was inclined to accept at [99] of that judgment (that the *Wednesbury* standard applied) related to disclosure under the duty of candour in legal or regulatory proceedings.

29 This means that the fact that no-one considered at the time whether it was necessary to disclose the fact that Ms Ali was the source of the information is not fatal to the Police. But the burden remains on the Police to demonstrate the need to disclose Ms Ali's identity as the source of the information she gave. When the data controller did not balance the relevant interests at the time of the disclosure, the weight to be accorded to its assessment of necessity will be lower, but it remains in principle open to the Police to show that the disclosure was necessary by *ex post facto* evidence.

30 In my judgment, the Police have failed to carry that burden in this case.

31 First, Ms Ali had repeatedly made clear the importance she attached to remaining anonymous as the source of the information she had provided. She had also been assured that her anonymity would be preserved. These were important starting points for any consideration whether to pass on her identity as a source of the information. They are also likely to be important to others considering making a disclosure to the police. But there is no evidence that anyone weighed in the balance the importance of her wishes, or the assurances she had been given, either at the time of the referral or afterwards.

32 Second, Mr Taylor accepted in evidence that crime reports were sometimes filed where the person providing the information was identified simply as the "reporting party". He made clear that he did not believe that he was required, under the procedures which then applied, to consider whether that could have been done in this case, and that there was no such consideration.

33 Third, there was no evidence to support the submission that the identity of Ms Ali as the source was necessary to provide accurate information to Luton as to the credibility of the report. Intelligence reports used by the police and other investigative agencies often contain assessments of the source's reliability without identifying the source. The referral could have said that the information came from "a reliable source with direct knowledge of the facts" or words to that effect. There was nothing to explain why such a descriptor could not have been used here.

34 Fourth, there was also no evidence to support the submission that the report could not have been anonymised without affecting the quality of the information it contained. The DASH form could not have been used, since its format makes clear that the person giving the information is the victim. But that did not mean that the information contained in it could not have been conveyed by means of an anonymised report. No consideration was given to doing this. There was no evidence to support the suggestion that anonymisation would have materially affected the speed with which the report was referred or the priority given to it by Luton.

35 Fifth, I do not accept that, even if the report had been anonymised, it would necessarily have been obvious who the source was. The information could in principle have come from a variety of possible sources. Even if suspicion might have fallen on Ms Ali, suspicion is different from knowledge. And even if it were suspected that the information came originally from Ms Ali, there is a significant difference between providing information directly to the police and providing information to someone else, who then passes it on to the police. That difference may be critical in a domestic context, where the person providing the information may justifiably fear repercussions if it comes to be known that she is the direct source of the information.

36 It follows that, in my judgment, the Police breached Article 5(1)(a) and (b) of the GDPR by passing on to Luton Ms Ali's identity as the source of the information she provided about her ex-husband.

37 Moreover, the Police have not established that it was necessary to make the referral to Luton (including her identity as the source of the information) without telling Ms Ali that it was doing so. This means that, even if I had found that the disclosure of the information to Luton was necessary, I would not have found it established that the data

was processed transparently. So, there would in any event have been a breach of Article 5(1)(a) of the GDPR.

38 I have reached these conclusions without needing to consider whether the IOPC report is admissible in these proceedings. That would not necessarily be a straightforward question: see by analogy *Rogers v Hoyle* [2014] EWCA Civ 257, [2015] QB 265. Its resolution does not matter here, because nothing in the IOPC report could conceivably assist the Police.

Misuse of private information

39 The fact that Ms Ali had informed the police about her ex-husband was information in respect of which she had a reasonable expectation of confidence. That expectation arose from the assurances she had been given on the telephone and the circumstances in which she gave the information to PC Webb. The information was of a private character. The only question is whether Ms Ali's reasonable expectation of privacy was outweighed by countervailing interests. In my view, it was not, for the reasons set out at [31]-[35] above.

Breach of confidence

40 In my view, this case is more appropriately analysed as a case of misuse of private information than breach of confidence. In any event, on these facts, I can see no material difference between the analysis required to establish liability for these two wrongs.

Article 8 ECHR

41 As noted above, the disclosure by the Police to Luton of Ms Ali's identity as the source of the information she provided constituted an interference with her right to respect for her private life, as guaranteed by Article 8(1) ECHR. For the reasons set out at [31]-[35], the Police have not established that the interference was necessary in a democratic society within Article 8(2). The disclosure was therefore contrary to s. 6 of the 1998 Act.

Submissions on causation and quantum

42 Mr Scott submitted that the claimant's distress at the passing of the information that she was the source of the information she gave was distinct from her distress at the subsequent unlawful disclosure of that information to her ex-husband by Luton's employee Rhully Begum. He invited me to attribute 50% of the distress to the first disclosure and 50% to the second, a conclusion which he said was supported by the expert report of Dr Mir, a Consultant Psychiatrist.

43 Mr Scott referred to three authorities on quantum: *Halliday v Creation Consumer Finance Ltd* [2013] EWCA Civ 333, [2013] 3 CMLR 4 (where £750 was awarded for a data protection breach); *Gulati v MGN Ltd* [2015] EWCA Civ 1291, [2017] QB 149 (where it was said that damages awards for misuse of private information should bear a "reasonable relationship" with awards in personal injury cases); and *ST (A Child) v L Primary School* [2020] EWHC 1046 (QB) (where Deputy Master Hill QC awarded damages of £1,500 for misuse of personal information in a case where there was

"limited evidence of direct impact" on the claimant). In the latter case, reference was made to the decision of Mitting J in *TLT v Secretary of State for the Home Department* [2016] EWHC 2217 (QB) (where awards of between £2,500 and £12,500 were made to asylum seekers whose details had been erroneously made public).

44 Ms Oborne opposed the admission of Dr Mir's report. There was no permission for expert evidence and, under CPR 35.4, no entitlement to rely on the report without permission. In any event, Ms Ali's pleaded claim is for damages for "psychological distress and anxiety", not the psychiatric injury identified by Dr Mir. Moreover, there was no evidence to show that any of the distress suffered by the claimant was caused by anything other than the disclosure to her ex-husband by Ms Begum. The disclosure to Luton gave rise to no distress or distress that was *de minimis* and so should give rise to nominal damages only.

Conclusions on causation and quantum

45 It is important to keep the claim under the GDPR separate from the claims for misuse of private information and breach of confidence.

The claim under the GDPR

46 In *Lloyd v Google* [2021] UKSC 50, [2022] 1 WLR 1217, at [138], Lord Leggatt (with whom the other members of the Court agreed) held that there is no right, whether under the Data Protection Act 1998 or the EU legislation which preceded the GDPR, to damages other than for material damage or distress. There is no reason to suppose that the position is any different under the GDPR.

47 In this case, the claim is for "distress and anxiety". But on a fair reading of the Particulars of Claim there is no pleaded claim for psychiatric injury; and I agree with Ms Oborne that Dr Mir's report should not now be admitted, no permission having been sought.

48 Ms Ali does not say that the disclosure in this case gave rise to pecuniary loss. The only basis for damages under the GDPR is, therefore, distress. I accept that Ms Ali suffered considerable distress as summarised in [12] above. Are the Police liable for any part of this distress?

49 On Ms Ali's own account, the distress which she felt arose when family and friends started asking her questions about whether she had gone to the Police about her ex-husband. This can only have been after, and because of, the disclosure by Ms Begum. On an orthodox analysis, the question whether the Police are liable for this distress depends on whether their breach of the GDPR caused that distress. Clearly the Police's disclosure to Luton was a "but for" cause. But that is not enough on its own. Consideration must be given to whether Ms Begum's actions broke the chain of causation. *Clerk & Lindsell on Torts* (23rd ed., 2020), at para. 2-114, suggests four questions relevant to that issue:

> "Was the intervening conduct of the third party such as to render the original wrongdoing merely a part of the history of events? Was the third party's conduct either deliberate or wholly unreasonable? Was the intervention foreseeable? Is the conduct of the third party wholly

> independent of the defendant, i.e. does the defendant owe the claimant any responsibility for the conduct of that intervening third party?"

50 A data controller who chooses to share personal data with another person or body may sometimes be responsible for damage flowing from negligent or even deliberate disclosure by that person or body, but much will depend on the circumstances. Here, the data was shared by a public authority with another public authority in the context of statutory duties owed by both and pursuant to a written agreement. In those circumstances, it may be fair to fix the first public authority with the consequences of a negligent disclosure by the second. It is not, however, fair to fix the first with the consequences of a deliberate, criminal breach by an employee of the second. In answer to Clerk & Lindsell's fourth question, the Police were not responsible to Ms Ali for Ms Begum's conduct. At the point of Ms Begum's disclosure, the earlier breach by the Police was merely part of the history of events. I would therefore conclude that Ms Begum's conduct broke the chain of causation.

51 It does not follow, however, that it would be fair for the Police to escape liability altogether. It is obvious from the evidence that Ms Ali was intensely concerned about that her identity as the source of the information should not be shared any more widely than necessary, even within the Police (as demonstrated by her request to the call handler not to say her name out loud). Even if there had been no disclosure by Ms Begum, Ms Ali would still have suffered some distress if she had been made aware that her identity as the source of the information had been passed to Luton. The Police would have been responsible for that distress. I can see no reason why the Police should be better off than they would have been in that situation merely because of Ms Begum's subsequent criminal disclosure.

52 I would therefore hold that Ms Ali is entitled to some compensation for distress under the GDPR. In my judgment, the appropriate sum is £3,000. I note that this is in the bottom half of the range of awards for "less severe psychiatric harm" in the *Judicial College Guidelines for the Assessment of General Damages in Personal Injury Cases* (16th ed.).

Misuse of private information

53 If the analysis in [51] above is wrong, compensation is available in the tort of misuse of private information on a wider basis than under the GDPR. In particular, a successful claimant is entitled to damages to compensate them for the loss or diminution of the right to control the use of their private information independently of any distress caused: *Gulati v MGN Ltd*, [45]-[48]; *Lloyd v Google*, [141]. If it were necessary to do so, I would award Ms Ali the same amount – £3,000 – as compensation for loss of the right to control the information that she was the source of what was communicated to the Police about her ex-husband.

Article 8 ECHR

54 If it were necessary to do so, I would award the same amount – £3,000 – for breach of Ms Ali's rights under Article 8 ECHR. There is some doubt about whether damages may be awarded for a breach of Article 8 where the breach has not given rise to some form of "mental harm" (see *Lloyd v Google*, [127]), but it is well established that compensation for breaches of Convention rights does not require the same strict

approach to causation of loss as is required for some common law torts. I am satisfied that, in the circumstances set out in [51] above, an award in the sum of £3,000 would be appropriate by way of just satisfaction.

Result

55 The claims for breach of Article 5(1)(a) and (b) of the GDPR, misuse of private information and breach of s. 6 of the 1998 Act succeed. There will be judgment for the claimant in the sum of £3,000.