NINESTJOHNSTREET

LARGE LOSS PERSONAL INJURY

GDPR & PERSONAL INJURY LITIGATION

5 November 2020

Brian McCluggage

brian.mccluggage@9sjs.com

INTRODUCTION

1. This short paper accompanies a short talk given on some features of how GDPR and the Data Protection Act 2018 may prove relevant to personal injury litigation.

2. There must be some initial caveats:

   a. Personal Injury is a broad field of practice;

   b. GDPR is largely unexplored in relation to its ancillary effect upon litigation.

3. Thus, my paper must be viewed as a series of musings rather than as an authoritative view on how issues would play out in practice.

4. It does seem that road traffic litigation involving personal injury (and its ancillary accoutrements such as credit hire claims, storage etc) is one field which may be replete with data issues. However, GDPR may have just as significant effect in catastrophic injury work, in which I practice day to day.

5. The GDPR is substantially concerned with privacy. Some primary features of the (very lengthy) Preamble to the Regulation include:

> The protection of natural persons in relation to the processing of personal data is a fundamental right. Article 8(1) of the Charter of Fundamental Rights of the European Union (the "Charter") and Article 16(1) of the Treaty on the Functioning of the European Union (TFEU) provide that everyone has the right to the protection of personal data concerning him or her.
>
> The processing of personal data should be designed to serve mankind. The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality. This Regulation respects all fundamental rights and observes the freedoms and principles recognised in the Charter as enshrined in the Treaties, in particular the respect for private and family life, home and communications, the protection of personal data, freedom of thought, conscience and religion, freedom of expression and information, freedom to conduct a business, the right to an effective remedy and to a fair trial, and cultural, religious and linguistic diversity.

6. One does not need to be eagle eyed or a connoisseur of human rights arguments to immediately realise the potential overlap with the article 8 Convention Right to Privacy.[1] As a brief reminder, a public body like the courts or public authority litigants must respect litigants' human rights: section 6, HRA 1998.

7. For busy personal injury lawyers, insurance claims handlers, and others involved in this type of litigation, there is a grave risk of overload. It is why 'human rights' points are rarely raised and considered rather esoteric – they just get in the way of getting through the evidence for many of us.

8. However, GDPR exists and may well have relevance to litigation.

9. While this talk revolves around issues within personal injury litigation it will raise concepts that may well be relevant to aspects of employment and commercial litigation. At the very least it may help with an understanding of how concepts may apply to evidence generally.

Coverage: Three Areas of Focus

10. Given the necessarily selective area of the talk and paper, I am going to focus on 3 areas:

    a. GDPR and use of surveillance evidence;

    b. GDPR and Medical Records;

    c. GDPR and Social Media.

11. Surveillance, Medical Records and Social Media are of course evidential subjects which frequently arise in personal injury litigation but also in other areas of law. It is not unknown for a disgruntled employer to seek to follow an employee signed off on sick or who is suspected to be in breach of restrictive covenants. Disciplinary action can arise out of social media posts.

12. Other "data issues" that can arise but which there will not be room to touch upon here will include:

[1] As enshrined in Schedule 1 to the *Human Rights Act 1998* incorporating the *European Convention on Human Rights*.

a. Insurance claim databases e.g. CUE, MIAFTR

b. Automatic numberplate recognition (ANPR): this is a 'hot topic' at present and to an extent too sensitive a topic to cover just yet. Obtaining information from police databases can be of great use in detecting fraud, whether that be in the context of a damaged vehicle being driven when it supposedly is not justifying a credit hire claim, or determining whether a claimant who asserts he is restricted to the house is out and about.

c. Personal injury suffered as a result of data breach. I am instructed in a case at present where a data breach is alleged in the aftermath of a serious accident, exacerbating psychiatric symptoms and potentially constituting a separate actionable breach of duty.

Where do the issues lie?

13. Dr Sorabji's talk will have set out the structure of the legislation, something he is truly an expert in. We will not rehearse the structure of the law here, but merely touch upon the basics as a reminder.

14. Section 2 of Data Protection Act 2018:

> 2 Protection of personal data
>
> (1) The GDPR, the applied GDPR [UK GDPR] and this Act protect individuals with regard to the processing of personal data, in particular by—
>
> (a) requiring personal data to be processed lawfully and fairly, on the basis of the data subject's consent or another specified basis,

15. Where one looks to processing "lawfully and fairly", the current data protection principles set out at Article 5 of GDPR are key. Personal data shall be:

> a) processed lawfully, fairly and in a transparent manner in relation to individuals;
>
> 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 not be considered to be incompatible with the initial purposes;

> c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed; [THIS IS STRICTER THAN UNDER THE 1998 ACT]
>
> d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
>
> e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and
>
> 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."

16. The words in section 2 only allow processing in the first place upon the data subject's consent or another specified basis. "Consent" will rarely be forthcoming from a claimant unless particularly co-operative (and must be active and explicit and given before the processing takes place). Thus we must look to other justifications.

SURVEILLANCE EVIDENCE

17. On now established principles of procedural law, covert surveillance need not be disclosed as part of the process of Standard Disclosure, but may be withheld and introduced at a later stage, after the claimant has asserted his positive case as to disability whether in witness statements, to experts or in a schedule of loss as the case may be.

18. In Rall v. Hume [2001] EWCA Civ 146, Potter LJ stated:

> "In principle, as it seems to me, the starting point on any application of this kind must be that, where video evidence is available which, according to the defendant, undermines the case of the claimant to an extent that would substantially reduce the award of damages to which she is entitled, it will usually be in the overall

> interests of justice to require that the defendant should be permitted to cross-examine the plaintiff and her medical advisors upon it, so long as this does not amount to trial by ambush."

19. In Ralls and in subsequent well-known cases such as Douglas v. O'Neill [2011] EWHC 6901, Hayden v. Maidstone NHS Trust [2016] EWHC 1121 and Stewart v. Kelly [2016] EWHC 3263, the emphasis was many much on assessing whether there was an 'ambush' rather than on any other relevant factor.[2]

20. That focus was also (at least in the later post-CPR cases) at the expense of any consideration of Denton principles. This I have always found slightly odd, because while surveillance material and logs are 'privileged material' and so did not have to be disclosed, they can only be formally proved by witness evidence. Generally, by the time surveillance is disclosed, the time for serving lay evidence has expired and so relief would need to be sought for the latter because of the standard 'debarring' order in the civil court's model directions.[3] Thus there is a sanction against which one would need relief under CPR Part 3.9.

21. The third principle of Denton is "all of the circumstances of the case so that the case can be dealt with justly". One could envisage that GDPR compliance might be involved as part of the argument in terms of a relevance circumstance and what ultimately is 'just'.

22. Section 57 of the Data Protection Act 2018 sets out general obligations of a data controller which include *implementing appropriate technical and organisational measures to ensure, and to be able to demonstrate, that the processing of personal data complies with the requirements of this part.*

23. This is will include implementing appropriate technical and organisational measures for ensuring that by default, only personal data which is necessary for each specific purpose of the processing is pursued [s.57(3) DPA 2018].

---

[2] There are cases where surveillance has been excluded because of 'lateness' leading to a perception of injustice e.g. Hicks v. Rostas [2017] EWHC 1344; O'Leary v. Tunnelcraft Ltd [2009] EWHC 3438

[3] i.e. "Oral evidence will not be permitted at trial from a witness whose statement has not been served in accordance with this order or has been served late, except with permission from the Court."

24. The duty applies to:

    a. The amount of personal data collected;

    b. The extent of its processing;

    c. The period of its storage;

    d. Its accessibility.

25. So the immediate question which arises is whether there is a breach of the DPA/GDPR if an insurer puts in place a loose and arguably excessive schedule of data collection:

    - Every day for two weeks?

    - Static surveillance (i.e. a fixed 'motion sensitive' camera) which can be put in place for weeks and show every time a data subject leaves and enters a property?

    - Following a claimant both on the street and into establishments such as a café or restaurants and monitoring every second of a private meal (albeit in a publicly accessible venue)?

    - Listening into conversations in the café or restaurant.

26. Is such surveillance compliant with the *3rd Data Protection Principle ie. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed?*

27. One can see where problems arise. What prospects might a claimant have to argue the following:

    a. Permission will properly be given by the court but only in respect of material that complies with the GDPR and thus certain parts should be excluded?

    b. Prior to knowledge of surveillance, seeking a direction that should insurers obtain any it must be GDPR compliant and 'kept up to date' i.e. such surveillance should not have an artificial cut-off date as might lead to an artificial selection (in other words, as soon as some useful material is obtained).

28. The argument would ultimately be that evidence which contravenes the GDPR should be excluded under CPR 32.1:

32.1

(1) The court may control the evidence by giving directions as to –

(a) the issues on which it requires evidence;

(b) the nature of the evidence which it requires to decide those issues; and

(c) the way in which the evidence is to be placed before the court.

(2) The court may use its power under this rule to exclude evidence that would otherwise be admissible.

29. How does the legislation apply to the following potentially problematic scenarios?

    a. Monitoring not so much the personal injury claimant him/herself, but support workers/carers where it is thought that an expensive care regime being funded by insurers is not in fact being implemented e.g. carers come to property 9am to 5pm, but claimant is out of property by himself from 11am to 4.30pm, leading to the implication that the carers are watching television or are acting as cleaners.

    b. Tracking vehicle movement e.g. a 'tracker' on the car.

    c. Surveillance of a claimant and member of her family in a private place e.g. back garden or through the living room windows

30. Jones v. University of Warwick [2003] EWCA Civ 151 is a leading case on admissibility of surveillance obtained through misleading and deceptive practices and may have some relevance here. A surveillance operative posed as a market researcher and was allowed into the claimant's home and covertly filmed her inside. The court balanced the claimant's article 8 right to privacy against the defendant's article 6 right to a fair trial and considered CPR Part 1.1 and 32.1. The evidence was considered so highly probative of the issues that the defendant was permitted to rely upon it, with a costs sanction being applied to the defendant, but only in respect of the admissibility proceedings.

31. It can immediately be observed that especially in an era of section 57 of the *Criminal Justice and Courts Act 2015* with dismissal of the entirely of an action on account of 'fundamental dishonesty', the costs to an insurance company of a few hearings dealing

with admissibility will be small beer compared with the saving on kicking out of the civil justice system a (potentially) six or seven figure case.[4]

32. However, if the claimant in a modern-day Jones situation was able to show that the data relating to her in her own home was processed 'unfairly' in reach of the first data protection principle, one might think that would be an important factor in the balancing of rights and perhaps more importantly application of the Overriding Objective.

33. The facts of the employment case XXX v. 1) YYY and 2) ZZZ [2004] IRLR 137 are instructive. A covert video was made by the nanny employee of the two respondents whom she worked for in context of sexual harassment allegations. The video showed both the male employer but also his son. Admissibility of the surveillance was argued by reference to article 6 and 8 Convention Rights. The claimant argued it showed that there was a consensual relationship between the nanny and the man of the house. The Employment Appeal Tribunal concluded that there was a serious interference with the Article 8 right to privacy of the child who featured and thus thought that the video should be seen by the Employment Tribunal at first instance but in private. As it happens the Court of Appeal ruled that the surveillance should not be used at all because it was irrelevant to the formal issues between the parties.

34. However, the seriousness of the breach of the child's Article 8 right to privacy and the suggested change of procedure does give encouragement that in serious breach cases a CPR Part 31 power could be used to exclude such evidence. The Court of Appeal had confirmed in Grobellar v. News Group Newspapers (1999) that CPR Part 32.1 allowed a court to exclude evidence that was otherwise both relevant and admissible.

35. Is the defendant/insurer required to carry out a Data Protection Impact Assessment under section 64 of DPA 2018 in respect of surveillance because it is a "type of processing … likely to result in a high risk to the rights and freedoms of individuals."

36. Could a claimant utilise rights under the DPA 2018 to raise a complaint to the Data Commissioner (ICO) under section 165 or to the court under section 167 which applies if "on an application by a data subject, a court is satisfied that there has been an infringement of the data subject's rights under the data protection legislation in contravention of that legislation". The court may make an order that the controller take

[4] I am only surprised that the decision in Jones v. University of Warwick did not encourage much more illicit behaviour.

steps or refrain from taking steps and may make an order of compensation for 'non-material damage' including distress

37. Other issues relevant to surveillance will be covered below when examining use of social media evidence.

MEDICAL RECORDS

38. Disclosure of medical records is such a commonplace occurrence in personal injury litigation that limitations in disclosure are nowadays simply ignored in practice.

39. There is an irony in the fact that objections were commonly raised to requests for wholesale disclosure of records in the 90s and to some extent in the 00s but have now been effectively given up despite increased emphasis on rights to confidentiality and data privacy.

40. As all who practice personal injury litigation know, disclosure of medical records can provide an abundance of evidential riches for the other party well beyond the injury or pathology at hand:

    a. A pre-existing history of the index condition;

    b. A medical history which contradicts that given to the medical experts in the case;

    c. Wholly unrelated conditions which may give rise to issues of causation e.g. an occupation would likely have been interrupted in any event;

    d. An insight into present complaints e.g. a history of somatoform type complaints/unexplained medical problems.

41. Sometimes material may simply be prejudicial:

    a. An aggressive temperament to doctors and nurses (which is always recorded);

    b. A drug habit;

    c. A past now forgotten: a previous occupation as a prostitute for example;

    d. A spell in prison.

42. Sometimes material may be more embarrassing than probative:

    a. Sexual dysfunction;

    b. Paternity issues;

    c. Sexual abuse;

    d. Psychiatric history generally, in any age where there may still be prejudice against 'hidden illness'.

43. Pre GDPR authority on disclosure of medical records is surprisingly thin on the ground.

44. In Dunn v. British Coal Corporation [1993] PIQR P275, the Court of Appeal decided that a defendant was entitled to disclosure of all of the plaintiff's medical records where he alleged a continuing and permanent loss of earnings and impaired earning capacity. The claimant had offered to disclose only records relevant to his neck injury and previous records showing neck pain. On the first appeal, the judge decided that relevance of wider records was to be decided by the clinicians who held the records. The Court of Appeal held that because other records might show that he would not have worked to normal retirement age, all records would be disclosed, but the order would be limited to the defendant's medical advisers in confidence except insofar as it was necessary to refer to matters relevant to the litigation. *Thus this was a very different sort of order and practice than one sees today, where lawyers have access to all records.*

45. In Hipwood v. Gloucester Health Authority [1995] PILR 447 the Court of Appeal discussed a hypothetical case of GP records containing evidence of a sexual disease but which a claimant had fully recovered from 20 years earlier. It was envisaged that the claimant's advisors might make an objection with the defendant asking its expert whether the record was relevant without seeing or being told of the substance of the record concerned.

46. In Bennett v. Compass Group [2002] EWCA Civ 642. The Court of Appeal held that the defendant was entitled to inspect the claimant's records but that an order should be carefully worded to ensure that the claimant's rights were not infringed, with a defendant only seeing the records in clearly defined circumstances with the precise nature of what was to be disclosed delineated.

47. The potential problem with this approach is that asking a defendant's experts to effectively determine what was relevant could be (a) time-consuming (b) expensive if records were voluminous (c) inadequate if the expert did not really know what he/she was looking for (given he is a doctor, not a lawyer).

48. The question is whether the GDPR and special treatment given to sensitive data might lead to either a different approach or a more nuanced approach than the present practice of indiscriminately disclosing every scrap of paper since birth under CPR Part 31.

49. It is useful to remind ourselves what CPR 31.6 says about standard disclosure:

> **31.6** Standard disclosure requires a party to disclose only–
>
> (a) the documents on which he relies; and
>
> (b) the documents which –
> (i) adversely affect his own case;
> (ii) adversely affect another party's case; or
> (iii) support another party's case; and
>
> (c) the documents which he is required to disclose by a relevant practice direction.

50. That wording would not obviously seem to support wholesale disclosure of medical records.

51. Article 9 of GDPR reads:

> 1. Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.
>
> 2. Paragraph 1 shall not apply if one of the following applies:
>
> (i) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;

(ii) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;

(iii) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

(iv) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;

(v) processing relates to personal data which are manifestly made public by the data subject;

(vi) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;

(vii) processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;

(viii) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;

> (ix) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;
>
> (x) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

52. Potentially relevant grounds justifying disclosure of health records which inherently contain "special categories of personal data" are underlined.

53. However, it is really only (vi) and (vii) which could be relevant.

54. Of note, (vi) relating to defence of a claim has no explicit 'balancing' requirement, whereas (vii) touching on substantial public interest does so.

55. However, the data principle of "data minimisation" [Article 5(1)(c)] would introduce proportionality and relevance back into the equation.

56. Thus, I submit that there is room for argument that restrictions as to wholesale disclosure of records are encouraged by the GDPR.

57. If a defendant wishes to see records, then preparation of an assessment (a LIA, see further below) and a data policy stressing security would probably promote a proposal to give disclosure of all records to the opposing solicitors. In days past, boxes full of medical records would be shipped around the country and necessarily left in chambers, taken to court in the boot of a car etc. In an age of (covid-enforced) paperless working, matters are very different. Passwords are extremely irritating but the one class of documents where they are probably most justified is on medical records, which will contain a class of documents far wider than the issues in the case and whose loss could be personally devastating to a litigant.

USE OF SOCIAL MEDIA AS EVIDENCE

58. What would seem an easy answer to any objection to use of a litigant's social media feeds is that it is in the 'public domain' and therefore fair game.

59. The problem with this is that it ignores that information from a social media feed is still likely to constitute "personal data" and so use is in principle governed by the GDPR.

60. What might be useful in relation to "personal data"? Having read many 10,000s of pages of litigants' social media feeds and found a few myself, the following come to mind taken from actual cases which I have conducted:

    a. Holiday photos (useful material in many contexts but invaluable in notorious holiday sickness claims), showing where a claimant is and what he is doing with friends and family;

    b. Sports activities (very handy when the disabled claimant is playing football or cricket in a team). One can then start to data mine the team and discover the number of appearances, what his teammates have been saying about him on Twitter etc.

    c. Ebay activity. This is less obvious but one can sometimes work out the ebay username from email addresses, usernames on Twitter etc, or even by undertaking geographical searches. This may show an unemployed claimant running a business on the side. Think that is unlikely? I have seen seven figures worth of damages destroyed by ebay. One case involved a busy home furniture refurbishing business; the other was a caravan letting business which the claimant alleged she played no part in because of her brain damage.

    d. Facebook: well, of course. But see Tuson v. Murphy [2018] EWCA Civ 1461 for how Facebook can lead to astonishing discoveries in terms of what has been going on behind the scenes.[5] A claim of £1.5 million future loss of earnings had been presented by a claimant suffering from an alleged severe OCD that left her barely able to leave the house because of an aversion to dirt, but was running a 'messy play' art class for infants and toddlers including at country fairs, village fetes etc.

[5] The case was not my happiest hour in terms of the result of the appeal on costs, but a claim pitched at approximately £2,000,000 was settled for £350,000 (pre section 57, as this would have been an obvious case of fundamental dishonesty).

Interestingly for present purposes, the claimant expressed herself in her witness statement to be "violated and disgusted" by the defendant's investigations and use of the social media material.

e. Twitter: comments between two users showing a propensity of a litigant to take recreational drugs which might be relevant generally to employment prospects of a prospective commercial pilot.

61. Social media evidence is perhaps a useful vehicle for considering whether **Article 6 of GDPR** has been complied with:

> 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.

62. Contrary to popular assumption, "Consent" is unlikely to be a good ground for lawful processing. This is because under the GDPR consent must be active and explicit and granted before the processing took place. A litigant might have placed photographs on Facebook for many purposes (ego, boastfulness, spite) but certainly not so that an insurance company could use the same in litigation.

63. So "legitimate interest" would likely have to constitute the appropriate legal basis. Relevant questions will be:

    a. What is the legitimate interest?

    b. Is the processing necessary to achieve that interest?

    c. Do the claimant's interests and fundamental rights and freedoms override the insurance company's interests in processing, which is a balancing test?

64. Has the insurer carried out a legitimate interests assessment ("LIA") to show that these have been complied with? Article 4(1) of GDPR requires the controller to "be responsible for and to be able to demonstrate compliance with paragraph 1" which includes of course that the processing is adequate, relevant and limited.

65. What immediately occurs to me is the number of times I have been provided with thousands of pages of largely irrelevant Facebook public postings not only of the claimant, but of his friends and family. If that material is sent to counsel (or by insurers to solicitors) without any screening for what is material to the issues in the case, then arguably there is a breach of GDPR.

66. Is that workable in the real world? Is there any real possibility of comeback? Generally a wad of irrelevant social media material would not be disclosable.

67. Fortunately, the ICO takes the view that any LIA only needs to be brief.[6] I would suggest it could be a few lines in a file note. The main thing is that fee earners dealing with these decisions are aware that they are supposed to consider it.

68. Legitimate interests would probably be:

    a. Business interest ie. to properly consider the claim made;

    b. To prevent and investigate fraud (see recital 47 of GDPR)

    c. Detection of Crime (see recital 50 of GDPR).

69. Is the processing 'necessary' in the sense of being 'proportionate' to the insurance company's interest? This may depend on the issues in the case. If the material was

[6] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/how-do-we-apply-legitimate-interests-in-practice/

likely to be of peripheral relevance or enquiries could be done in a different way, then it may well not be necessary.

70. Assuming that is met, ICO guidance on the balancing test states that three things need to be considered in carrying out this test:

    i. the nature of the personal data to be processed;

    ii. the individual data subject's reasonable expectations;

    iii. the likely impact of the processing on the individual and whether any safeguards can be put in place to mitigate negative impacts.

71. It seems to me that the claimant's interests and rights might be thought to be limited where postings have been made publicly available, which subject to privacy settings, is often the case. In defamation cases, it seems well established that comments made in a setting which allows the public or any friend to read from 'the wall' is 'publishing' it no different from placing comments on an office notice board: see Stocker v. Stocker [2018] EWCA Civ 170.

72. The test for 'reasonable expectations' is at least objective (GDPR Recital 47).

73. Holiday photographs on a public Facebook wall may be 'easy' but what about the following significantly more difficult scenarios?

    a. Where a litigant's Facebook/Twitter is set to private, but a disgruntled friend or workplace colleague is prepared to 'leak' material to the other side, whether that be posts made available to friends only or a set of private messages. *This is not too good to be true – it happens often if intermittently in litigation.*

    b. Where a false identity is used to 'befriend' the litigant to get access to private posts (*analogous I suppose to the* Jones v. University of Warwick *case discussed in the surveillance section above*).

    c. Where not a false identity as such but a 'generic profile' is set up that has the same effect. For example, if one knew that a litigant with a private Instagram account was interested in, say, vaping, an account could be set up saying "Vaping Ideas" which just reposted lots of vaping photographs available from Pinterest or similar. A litigant might accept a friend request from such a source.

74. The argument would run that social media material not publicly available but given confidentially or which has been obtained through a misleading profile should be excluded.

75. One can see that in a balancing of respective rights and interests, this may not be 'necessary' for the legitimate interest. A litigant might ask the court to exclude the material on that basis under CPR Part 32.1 in conjunction with the Overriding Objective due to breach of the GDPR.

76. Against that it might be argued on behalf of the other party:

    a. The litigant was herself prima facie guilty of deception as shown by the photos.

    b. There is a lot of money at stake.

77. Other countervailing factors:

    a. Is the material embarrassing or humiliating (e.g. 'dirty pics')

    b. Does it betray irrelevant criminal behaviour;

    c. Might it interfere with family relationships (e.g. disclosing an affair, but which is tangentially relevant to the case).

78. Sometimes the social media material might involve special category personal data i.e. health data. One will then be considering issues as were raised above in context of medical records. It is here we are considering in order to make lawful:

    a. Article 9(2)(e): where "processing relates to personal data which are manifestly made public by the data subject" – *so an open profile will be particularly important here.*

    b. Article 9(2)(f): where "processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity"

    c. Article 9(2)(g): substantial public interest, proportionate to the aim pursued.

79. Where might the difference lie between personal data under Article 6 and health data under Article 9? Article 9 uses the language of 'prohibition' unless one of the exceptions is allowed. Article 6 uses the expression, "processing only if and to the extent that" the various threshold conditions might apply. There appears to me a

substantive difference between "legitimate interests pursued by the controller" in Article 6 and "substantial public interest" of Article 9, the latter requiring something more weighty.

80. The "defence of legal claims" seems in some ways the easy get out option, but only if proceedings are underway. Pre-proceedings, where health data obtained from social media is concerned, one would need to rely upon 'substantial public interest. ICO guidance is to the effect that one would need to set out *"specific arguments about the concrete wider benefits' of the processing e.g., how it 'benefits the public in terms of both depth (ie the amount of benefit experienced from the processing, even if by a small number of people) and breadth (the volume of people benefiting from the processing).'*[7]

81. Where there is a real basis for thinking a claim might be fraudulent this should be satisfied; if one is merely 'fishing', establishing public interest should be more challenging.

82. The practical question is this: if the other side challenged your client's rights to rely upon the social media evidence because of GDPR how well placed will you be to answer that challenge?

BRIAN McCLUGGAGE

6 November 2020

[7] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/special-category-data/what-are-the-substantial-public-interest-conditions/