Additional material for chapter 28

Data Protection

Order protects media disclosures

The Data Protection (Processing of Sensitive Personal Data) Order 2000 (SI 2000/417) is a statutory instrument which sets out 10 circumstances in which ‘sensitive personal data’ may be lawfully processed. Several require that the processing is ‘in the substantial public interest’. For journalists the most important is in paragraph 3, which covers disclosures for journalistic, artistic, or literary purposes of personal data relating to:

- the commission by any person of any unlawful act (whether alleged or established);
- dishonesty, malpractice, or other seriously improper conduct by, or the unfitness or incompetence of, any person (whether alleged or established); or
- mismanagement in the administration of, or failures in services provided by, any body or association (whether alleged or established).

These and other parts of this instrument provide what are in effect ‘public interest’ defences as regards the processing of data.

Why did this statutory instrument not provide a defence to the Daily Mirror in the case - see McNae’s, p 360 - concerning Naomi Campbell? Remember that processing of data must also be ‘fair and lawful’. As the House of Lords reached the decision that the Daily Mirror coverage of Naomi Campbell’s therapy for drug abuse was a breach of confidence, it could not be said to be ‘lawful’.

Exemptions for the media

Section 32 of the Act says that personal data which are processed only for ‘special purposes’ (journalistic, literary, or artistic purposes) are exempt from some provisions of the 1998 Act, including those relating to:

(1) the data protection principles (except for requirements to keep data secure) - (2) subject access, which is explained below.

According to the Act, the section 32 exemption applies if the processing is undertaken ‘with a view to publication’ of special purposes material. But in the Campbell case the Court of Appeal said the exemption did not apply only to the period before publication. This means the exemption does not expire as a result of publication, and therefore that the law does not require a media organisation (‘as data controller’) to order its journalists to delete - or release in response to a ‘subject access request’ - information gathered for journalistic purposes about a person just because some of it has been published.

The exemption also applies only if the media organisation reasonably believes that:

(1) having regard in particular to the special importance of the public interest in freedom of expression, publication would be in the public interest; and
(2) in all the circumstances, compliance with the rules in the 1998 Act is incompatible with the journalistic purposes.

A freelance journalist, too, is a ‘data controller’ in respect of personal data about other people which he/she ‘processes’ (holds) - for example, on a laptop or memory stick.

Section 32 says that when considering whether a ‘data controller’s’ belief that publication would be in the public interest is reasonable, the court may pay regard to its (or his or her) compliance with ‘any relevant code of practice’. So it might weigh in a media organisation’s or the freelance’s favour if material
held or published was of a type covered by the public interest exceptions in either the Editors’ Code of Practice or the Ofcom Broadcasting Code, explained in McNae’s chapters 2 and 3, and which cover, for example, the exposure of crime or other wrongdoing. However, as these codes note, these are not comprehensive definitions of the public interest.

It can be argued that a journalist needs, in the public interest, to hold general background information about people who may figure in future news stories, not just those who already are or may be the target of an investigation.

**Protection of sources**

People have the right under the Act to discover whether a ‘data controller’ holds information about them, and, if so, what it is. This is known as a ‘subject access request’. They must also be told the purposes for which it is held - for example, journalism - to whom it is or may be disclosed; and the source of the information.

A person may send a subject access request to a media ‘data controller’ to attempt to find out, by asking for information about himself/herself, the source of a journalist’s information. In some circumstances the very nature of such information, to a requester who gets hold of it, might make the identity of the source obvious, so for the journalist to reveal any of it would betray that source. But a ‘data controller’ has the right not to comply with an access request if the material is held for ‘journalistic, literary, or artistic purposes’ and so is covered by the section 32 exemption. If the information is held for other purposes, the Act says the access request must be complied with, even in the absence of the other individual’s consent (that is, the consent of the source of the information) if it is reasonable in all the circumstances to comply without that consent.

**Case study:** The *Mid Devon Gazette* published a story about how Cullompton Town Council had held finance meetings in private, against regulations. It was written after a copy of a council email was leaked to the paper. The council and a former town councillor, Ashley Wilce, who had been denied access to a meeting, asked the paper for a copy of the email, but the Gazette refused because this could have led to its source being identified. Mr Wilce complained to the Information Commissioner’s Office, saying that the Gazette was breaching the Data Protection Act in its refusal. The paper, to justify its position, told the ICO that under section 32 of the Act it had an exemption in respect of data held for journalistic purposes and used in the public interest. The ICO case officer later told the paper the investigation into the complaint had closed, because ‘it is likely that the Mid Devon Gazette has complied with the requirements of the Act’ (*Holdthefrontpage*, 19 July 2012).

Lawyer Heather Rowe, a data protection expert, summing up the 1998 Act’s complex law for *McNae’s*, has this advice for journalists: ‘To my mind the provisions all say, taken together, that you do not have to name a source unless there is something like a court order that makes you do so.’

As *McNae’s* chapter 34 explains, if a court orders a journalist to identify a source, the journalist or his/her editor may make an ethical decision to defy the court and face the legal consequences.

**Powers of entry and inspection**

The 1998 Act gives the Information Commissioner wide powers of entry and inspection in relation to data held by data controllers. These powers can be exercised only under a warrant granted by a circuit judge (in Northern Ireland by a county court judge). A judge must not issue a warrant relating to personal data processed for the ‘special purposes’ (including journalism) unless the Commissioner has decided whether such data fall within the special purposes exemption.

As yet, there has been no example of the Commissioner ‘raiding’ the premises of media organisations for material being held (‘processed’) for journalism.
Guidance issued to the media on data law

Lord Justice Leveson, in his report into ‘the culture, practices, and ethics of the press’ (see McNaes’s chapter 2) recommended that the Information Commissioner should issue ‘comprehensive good practice guidelines and advice on appropriate principles and standards to be observed by the press in the processing of personal data’. Leveson said: ‘The Operation Motorman “treasure trove” constituted evidence of serious and systemic illegality and poor practice in the acquisition and use of personal information which could have spread across the press as a whole.’ Operation Motorman was the inquiry - referred to in McNaes’s, pp. 358-359 - which led to the conviction of private investigator Steve Whittamore for breach of the Act. His clients included several national newspapers.

In September 2014 the Commissioner, responding to Leveson’s report, issued the document ‘Data Protection and Journalism; a guide for the media’ – outlined in McNaes’s, p. 362.

The guide says its purpose ‘is to help journalists, editors, and managers understand and comply with data protection law and good practice, while recognising the vital importance of a free and independent media.’

It gives reassurance that a media organisation or journalist faced with a ‘subject access request’ can remove from the requested material the identity of confidential sources ‘as long as it is reasonable to do so.’