Additional Material for Chapter 34 – The Journalist's Sources

Section numbers from the book are used. Its content provides fuller explanations and context.

34.2.2 Court orders to name or produce material which could identify a source

A journalist protecting a source's identity may face a long and tortuous legal battle.

Case study: In 2000 Ashworth High Security Hospital obtained a High Court order that the *Daily Mirror* should disclose how it came to be in 'possession or control' of medical records – whether originals, copies or extracts - kept at the hospital on Moors murderer Ian Brady. He was a patient there. The hospital had applied for the order because a *Mirror* article included verbatim extracts of Brady's records. The High Court order was also that the *Mirror* must identify any employee of the hospital and the name of the person or persons (and any address, telephone and fax numbers known for such a person or persons) who were involved in the *Mirror* acquiring possession or control of these records. Brady was, at the time the article was published, engaged on a well publicised hunger strike protesting at being transferred from one ward to another and the manner of the transfer. The article was about this, and referred to what his records said about weight loss and his interactions with staff. The hospital's legal action against the *Mirror* started a case which lasted six years. The hospital, suspecting that the medical information about Brady had been disclosed by a staff member, intended to discipline – which in practice would mean dismiss – that person once he or she was identified, because of his or her breach of confidence in leaking the records. For the law of confidence in such contexts, see 26.2 and 34.7 in *McNae's*. The evidence of Gary Jones, the *Mirror's* investigations editor, who wrote the article, was that he received the extracts via an intermediary - who was paid £1,500 by the *Mirror* for them - and suspected the intermediary's source was a staff member at the hospital, whose identify Mr Jones did not know. Mr Jones, who was described by the High Court judge as 'a straightforward witness, explained that, in accordance with his normal working practice, he had destroyed the material that he had received after writing his article. The hospital's arguments that the source should be identified included that if its staff or patients felt there was a possibility of what was entered in patients' psychiatric records improperly entering the public domain, the staff's reporting in those records would be inhibited, patients would be deterred from providing information about themselves and there would be damage to patient-doctor relationship, which rests on trust. The hospital also argued that such a situation may lead to assaults by patients on a patient about whom information is disclosed in the media, create an atmosphere of distrust amongst staff - which would be detrimental to efficient and co-operative work - and give rise to fear of future (and potentially more damaging) leaks. The *Mirror* and Jones did not identify the intermediary source. The *Mirror* appealed to the Court of Appeal against the order, referring to the Article 10 rights of the media to have confidential sources of information. The *Mirror* also argued that Brady had already himself put the relevant medical information in the public domain. The hospital continued in the legal action to seek the identification of the intermediary source, hoping that would lead to the identification of the leaker of the extracts from Brady's records. The Court of the Appeal upheld the High Court's order against the *Mirror*, and the House of Lords (what is now the Supreme Court) upheld that decision, saying in 2002 that, while disclosing

sources had a 'chilling effect' on freedom of the press, the order was 'necessary and proportionate and justified' to protect the confidentiality of the hospital's medical records (*Ashworth Security Hospital v MGN Ltd* [2000] EWCA Civ 334, [2002] UKHL 29; [2002] 4 All ER 193). Freelance journalist Robin Ackroyd then said he was intermediary source who had supplied the extracts to the *Mirror* – but refused to identify his own source. The High Court ordered him to do so. But in May 2003 the Court of Appeal upheld his appeal against the order and ruled there should be a full trial of the issue, saying he had an arguable defence – the Court now knew, as the earlier court had not, that the person who gave Mr Ackroyd the information for his story was not paid for it. It said that if that individual had a public interest defence to any breach of confidence or contract claim by the hospital, a claim could not succeed against Mr Ackroyd. The Court of Appeal also said it did not automatically follow that the public interest in non-disclosure of medical records should override the public interest in maintaining the confidentiality of his source (*Mersey Care NHS Trust v Robin Ackroyd* [2003] EWCA Civ 663). At the High Court trial, in February 2006, Mr Justice Tugendhat, in these changed circumstances, rejected Ashworth Hospital's argument that the need to protect the confidentiality of medical records overrode the public interest in protecting a journalist's sources (*Mersey Care NHS Trust v Robin Ackroyd* [2006] EWHC 107 (QB)). The hospital appealed but the Court of Appeal found for Mr Ackroyd in February 2007 *(Mersey Care NHS Trust v Robin Ackroyd [2007] EWCA Civ 101*).

Other detail about the 2016 Act

As outlined in 34.3 in *McNae's*, the Investigatory Powers Act 2016 sets out law empowering the intelligence agencies and police to secretly intercept people's communications, and to extract information from computer systems and people's devices secretly or otherwise; and empowering these and other public authorities to secretly access people's communications data. Before the Act was created, these types of powers were provided in different statutes. The Government's justifications for the Act include that this new and consolidated law was needed to help identify and catch terrorists and other criminals, and to protect national security.

When the Act was being created, lobbying of Parliament by groups concerned about civil liberties, including media organisations, improved to some extent its safeguards for such liberties, including privacy in communications. Journalists were concerned, in particular, to protect their rights under Article 10 of the European Convention on Human Rights to have, and to protect from identification by officialdom, confidential sources of information - for example, people whose identity is unknown to police or other official agencies. These Article 10 rights enshrine 'the public interest' in there being some protection in law for 'whistleblowers' – for example, those seeking through journalists to warn the public of wrongdoing or inefficiency in the work of the police or other official institutions. See 34.2 in *McNae's*.

Concerns held by journalists were aired when the Act, as a Bill, was debated in the House of Lords. One peer warned that such law would permit state agencies such as the police to access, when trying to identify a journalist's confidential source, a journalist's notes or video footage stored on their phone, or to use its microphone as a bug. See Useful Websites, below.

The Act contains some safeguards – outlined below - to uphold journalists (and sources') Article 10 rights in respect of when police, intelligence services or other public authorities can use their powers to seek to identify such sources, including by gaining access to 'confidential journalistic material' in communications or computer systems. The law is that use of such powers for that purpose is only justified 'if this is necessary in a democratic society because of an over-riding requirement in the public interest'. This means that for each such use of these powers to be lawful there must be a particular circumstance, such as a need to protect national security or to prevent serious crime, which amounts to a public interest requirement stronger in law than the public interest in the journalist being able to keep secret the identity of a confidential source. Also, the law says that officialdom's use of investigative powers for that purpose must be 'proportionate'. For context about the law on 'over-riding requirement', and the proportionality principle, see 34.2 in *McNae's*.

When stressing the existence of Article 10 safeguards in the Act, the Government placed great weight on the roles created in this legislation for 'Judicial Commissioners' to approve or not approve warrants for police or intelligence services to intercept communications or to extract information from devices or computer systems, or to approve or not approve authorisations for these and other public authorities to gain access to communications data. Those roles are outlined below. There are 15 of these Commissioners. They are current and or recently retired High Court, Court of Appeal and Supreme Court Judges. As indicated in 34.3 in *McNae's*, because the Act permits these approval functions to be conducted in secret, there is little scope in law for any journalist who is subject to such authorised, official probing for the identity of a confidential source, or who fears it may have occurred, to know if it has occurred or any detail of how the Commissioners weigh up factors in their decisions on whether to approve it. But, as outlined above, the Commissioners' role in this respect is to ensure that the 'over-riding requirement' exists in law to justify each such approval, and that if it does, any probing of the journalist's communications, communications data and records will be 'proportionate'.

Note that when this Additional Material was completed, some law in the 2016 Act had yet to come into force to transfer to these Commissioners some roles held under other law by earlier types of commissioner.

A basic safeguard in the Act is that it has definitions of 'journalistic material' and 'confidential journalistic material' (definitions present too in earlier law). Section 264 defines 'journalistic material' as material created or acquired for the purposes of journalism, and 'acquired' means it was received by one person from another who intended that recipient to use it for the purposes of journalism. The section says material is not to be regarded as created or acquired for the purposes of journalism if it is created or acquired with the intention of furthering a criminal purpose (such as, for example, terrorism). The section says (here summarised) 'confidential journalistic material' in the case of material contained in a communication is journalistic material which the sender of the communication holds in confidence, or intends the recipient, or intended recipient, of the communication to hold in confidence; or in any other case, is journalistic material which a person holds in confidence.

34.3.1 Interception of communications

The Investigatory Powers Act 2016 consolidates and updates powers available to the police and intelligence services to 'intercept' - and so obtain what is said or written in – phone calls, texts, emails, letters and other types of communications. The Home Secretary can issue a warrant authorising such interception in the interests of national security, for the purpose of preventing or detecting serious crime, in the interests of the economic well-being of the United Kingdom so far as those interests are also relevant to the interests of national security, and at the request of other nations with which the UK has 'mutual assistance' agreements for such investigations.

The Act also enables the Home Secretary to authorise 'bulk' interceptions by intelligence agencies of 'overseas related' communications, even those of people not suspected of any crime, in the interests of national security, for the purpose of preventing or detecting serious crime, and in the interests of the economic well-being of the United Kingdom so far as those interests are also relevant to the interests of national security. This means that the content of thousands of such communications can be swept up by the intelligence services to be examined and analysed.

Sections 28 and 29 of the Act specify that when the police or an intelligence agency wants the Home Secretary to approve interception and/or examination of communications which the police or agency believes will contain confidential journalistic material, or when the purpose or one of the purposes of the interception or examination is to identify or confirm a source of journalistic information, the application for such a warrant must (to make the Home Secretary aware of this sensitivity) include a statement making clear this context or purpose for the application.

The sections also require specific arrangements to be in place for the handling, retention, use and destruction (when no longer needed for the investigation) of communications containing such material or which identify sources of journalistic material.

Under the Act, all interception and examination warrants must also be approved too by a Judicial Commissioner unless the Home Secretary or his/her deputy issued the warrant in urgent circumstances, in which case a Commissioner has to review that decision later.

Section 154 of the Act says that if a communication which has been intercepted in accordance with a bulk interception warrant is retained, following its examination, for purposes other than the destruction of the communication, and it is a communication containing confidential journalistic material, the person granted the warrant must inform the Investigatory Powers Commissioner as soon as is reasonably practicable. See Useful Websites, below, for more information about the role of this Commissioner and the Judicial Commissioners.

34.3.2 Probing of communications data

The 2016 Act also 'updated' powers the police and intelligence agencies, and a range of other public authorities to have targeted access to communications data – for example, by requiring telephone and internet service companies to provide it. Such data is not the content of a communication but information revealing who initiated/sent it, who the other party/recipient is, when and where it was made/sent, etc - see 34.3.2 in *McNae's*. Such access – for example, to data of phone calls or of email

traffic - can be authorised by a designated official in that authority for the purpose(s) the Act permits for that authority.

For example, the intelligence services can legally access the data in the interests of national security and in the interests of the economic well-being of the United Kingdom so far as those interests are also relevant to the interests of national security. The widest use of these powers is reserved for police forces. The intelligence services and police are by far the biggest users of these access powers.

As specified in the Act, other types of public authority can only legally access communications data as relevant to their function. For example, local ambulance trusts and fire and rescue authorities can access it only for the purpose of preventing death or injury or any damage to a person's physical or mental health, or of mitigating any injury or damage to a person's physical or mental health. Other purposes specified by the Act, according to each authority's function, as justifying access to such data include when this is in the interests of public safety, or to protect public health, or to assist official investigations into alleged miscarriages of justice, or to assess or collect any tax, or to exercise functions relating to the regulation of financial services and markets. There are particular, restrictive procedures in the Act for local authority councils who want to access communications data. But many of the authorities listed in the Act can legally acquire communications data for the purpose of preventing or detecting crime. And those that do not have this power can ask the police to investigate an alleged crime, which may be done by police accessing such data. So the law gives wide scope for public authorities to seek to justify accessing communications data to try to identify a journalist's confidential source in circumstances when a leak of information to the journalist by such a source is alleged to be criminal itself – for example, misconduct in public office or breach of data protection law - or when it is asserted that identification of such a source is necessary to investigate other crime. See 34.2 and 34.3 in *McNae's* for context, including that a Judicial Commissioner must approve authorisations to access data for the purpose of identifying a source of journalistic information.

> **Case study**: In January 2017 the Investigatory Powers Tribunal, a type of court with a duty to consider complaints about accessing of communications data, ruled that use of RIPA in 2012 by Cleveland police to access the communications data of two of its officers (who later became the complainants to the Tribunal), a solicitor, and three *Northern Echo* journalists was unlawful and excessive. Cleveland police were investigating leaks of information to the media about an officer's grievance case, a report about racism within the force and a murder inquiry. Among the Tribunal's findings were that the journalists' Article 10 rights were not considered before the authorisations were given, and there was insufficient consideration of whether the use of RIPA was proportionate (Case reference [2017] UKIPTrib15_586-CH).

As explained in 34.3.3 in *McNae's*, the relevant law in RIPA about targeted access by public authorities to communications data is due to be replaced by parts of the Investigatory Powers Act, referred to above, which when this Additional Material was written were not in force. Check www.mcnaes.com for updates.

34.3.4 Information stored in networks or equipment

The 2016 Act enables the Home Secretary to approve warrants for intelligence and law enforcement agencies, including the police, to conduct 'equipment interference' to get information stored in devices or systems, including computer networks, and to examine such information. For applications for this type of warrant, the Act's sections 113 and 114 created same type of safeguards as apply to the applications for interception warrants, see above. These include that if a purpose of the warrant is to obtain or examine communications or other items of information which the applicant for the warrant believes contains confidential journalistic material, or to identify or confirm a source of journalistic information, the applicant must tell the Home Secretary this in a written statement. Again, all of these types of warrant must be approved too by a Judicial Commissioner, unless the need for the warrant is urgent.

Codes of Practice

Under the 2016 Act's schedule 7 the Home Secretary is obliged to issue codes of practice for relevant officials to consider when deciding whether to seek warrants or authorisations or make authorisations based on the Act's powers; and for the Judicial Commissioners, the Investigatory Powers Commissioner, the Investigatory Powers Tribunal and any other court or tribunal to use when making or scrutinising decisions under the Act. Such decisions by a Judicial Commissioner could be, for example, whether to approve interception of communications or access to communications data to help the police or intelligence services identify a journalist's confidential source. The Investigatory Powers Commissioner has power to retrospectively review such decisions. Under schedule 7 each code must include provision to protect the public interest in the confidentiality of sources of journalistic information. Again, for context about the Investigatory Powers Commissioner and the Investigatory Powers Tribunal, see 34.3 and 34.4 in *McNae's* and Useful Websites, below.

The codes relevant to interception of communications, equipment interference, bulk acquisition of communications data, and intelligence services' retention and use of bulk personal datasets were approved by Parliament in 2018. These codes say: 'There is a strong public interest in protecting a free press and freedom of expression in a democratic society, including the willingness of sources to provide information to journalists anonymously.' They include emphasis on the need to comply with the proportionality principle – see 34.2.1 in *McNae's*.

The codes also say: 'An assessment of whether someone is a journalist (for the purposes of the Act) should be made on all the facts and circumstances available at the time. Consideration should be given, in particular, to the frequency of the individual's relevant activities, the level of personal rigour they seek to apply to their work, the type of information that they collect, the means by which they disseminate that information and whether they receive remuneration for their work. This approach will take into account the purpose of the provisions contained within the Act which is to protect the proper exercise of free speech, and reflect the role that journalists play in protecting the public interest.'

The codes say too: 'The fact that a person uses social media tools to communicate does not, in itself, indicate that that person is a journalist or that he or she is likely to be holding confidential journalistic material ...'

Other relevant parts of the codes include:
'Confidentiality can continue to attach to confidential journalistic material when it is sent to or held by a person who is neither the journalist nor the source (for example, a news editor who has been sent some notes by a journalist).'

'A source of journalistic information is an individual who provides material intending the recipient to use it for the purpose of journalism or knowing that it is likely to be so used. …..any reference to sources should be understood to include any person acting as an intermediary between a journalist and a source.'

For these codes see Useful Websites, below.

Monitoring of internet use
Journalists concerned about the potential for state surveillance and monitoring of their activity should note too that the 2016 Act requires internet companies to keep for 12 months data showing what websites people have visited, so it can, for example, be analysed in police investigations**.**

34.4 Be prepared to be watched or bugged

A journalist may be put under covert surveillance by an official agency wanting to know who his or her sources are – see too 34.4 in *McNae's.*

The Regulation of Investigatory Powers Act 2000 (RIPA) sets out how covert surveillance by official agencies – for example, police watching or 'bugging' suspected criminals - can be authorised.

It could, for example, be deemed lawful for police to watch or bug a journalist to discover who is leaking information to him or her from an official institution if that leaking is regarded as a crime. But, again, the Article 10 rights of the journalist (and source) mean there would have to be an 'over-riding requirement in the public interest' to justify the surveillance – for example, the suspected crime would need to be sufficiently grave for such surveillance to be lawful. And the principle of proportionality means, for example, that other steps to discover the source's identity should have been tried first.

The Act defines surveillance as 'directed' or 'intrusive'. 'Intrusive surveillance', for the purposes of the Act, is covert and involves use of a surveillance device (for example, a microphone or camera), or the presence of a person doing the surveillance, in residential premises or a private vehicle. Any other method of surveillance is described as 'directed', no matter how intrusive it is.

Under RIPA, authorisation for intrusive surveillance, which must be given by a 'designated' person (for example, a chief constable) must normally be approved too by a Judicial Commissioner unless the need for the surveillance is urgent, Some surveillance, including entry into and interference with

property, can in some circumstances be authorised by the Home Secretary with warrants issued under the Intelligence Services Act 1994 or the Police Act 1997.

Schedule 1 in RIPA gives a lengthy list of public authorities whose 'designated' representative can authorise directed (but not intrusive) surveillance. For example, councils can undertake such surveillance to try to catch those illegally dumping dangerous waste or on people suspected of fraudulently claiming benefits, if a magistrate approves the surveillance.

For the codes of practice for those authorising surveillance, see Useful Websites, below. The codes set out the safeguards in law for the protection of journalists' confidential material and the identity of their confidential sources. For example, the application for approval to conduct surveillance should state that the purpose is to discover the identity of such a source, to ensure that whoever is due to approve it is aware of this sensitivity. The definition of a journalist in these codes is the same as in the codes for those authorising interception, extraction, etc – see above.

The remit of the Investigatory Powers Commissioner includes oversight of the use of surveillance powers. For example, the Commissioner, in the event of discovering or being notified of any 'serious error relating to a person who has been subject to an investigatory power', has a duty to inform the person about the 'error', if doing that is 'in the public interest' and in those circumstances the Commissioner can also tell the person of their right to report the matter to the Investigatory Powers Tribunal.

34.5 Article 8 rights to privacy and private life

Case study: A warrant for a search of a newspaper's office issued by a Luxembourg court breached both Article 8, covering the right to respect for privacy and family life, and Article 10, guaranteeing the right to freedom of expression, of the European Convention, the European Court of Human Rights held. The fifth section chamber of the court considered the issue of protection for journalists against coercive court orders in the case of *Saint Paul Luxembourg SA v Luxembourg* (Case No 26419/10) in a decision handed down on 18 April 2013. A warrant to search a newspaper office was, in the circumstances, a violation of Article 8 and, because the warrant was in wide terms which potentially included information about sources, also a violation of Article 10, the court said. The case came after *Contacto Semanário*, a Portuguese language newspaper published by the applicant to the Court, printed in December 2008 an article about families losing custody of their children. The piece was signed by Domingos Martins - a name which did not appear on the list of Luxembourg press council journalists, although it did have a journalist named Alberto De Araujo Domingos Martins. A defamation complaint was made and a criminal investigation opened. In March 2009 a search warrant was issued to obtain documents in relation to these offences, including in relation to the identification of the author of the article. The warrant was executed and the journalist gave police the relevant documents, and journalist and the applicant's staff cooperated with the police during the search. But the applicant subsequently applied, unsuccessfully, to the domestic court for an order cancelling the search warrant. The applicant contended that the search of the premises of the newspaper was a violation of Article 8 of the Convention. In its

judgment the fifth chamber court rejected the notion that Article 8 only protected the 'homes' of individuals. The term 'home', it said, 'should be interpreted as also including the official office of a company run by an individual, and the official office of a legal person, including subsidiaries and other business premises.' The fact that journalists and staff co-operated with the police did not deprive the search and seizure of its intrusive nature. If there had been no cooperation the police would have executed the warrant in any event. As a result, it was clear that the search was an interference with the applicant's Article 8 rights. The exceptions in Article 8 had to be interpreted narrowly, and the necessity for them in a given case had to be convincingly established, the court said. Although the purpose of the search was supposed to be to identify the author of the article, the connection was obvious from the published list of journalists. 'On the basis of these elements, the investigating judge could have - as a first option - taken a less restrictive measure to confirm the identity of the author of the article, rather than issuing a search and seizure order. The search and seizure were, therefore, not necessary at this stage', the court said. As a result, the search and seizure was not proportionate and was not justified under Article 8(2). In relation to Article 10, the broad wording of the order did not exclude the possibility that it would be used to obtain information about the journalist's sources. Although the Luxembourg Government said the sources were not being sought, information about them could have been obtained under the warrant. As a result, the court said, the search was disproportionate and there was a breach of Article 10 as well.

- *McNae's* authors are grateful to Hugh Tomlinson QC and the Inforrm blog for their permission to use, in the text above about the *Saint Paul Luxembourg SA* case, an edited version of an article about which first appeared in Inforrm on 17 May 2013.

34.6.2 Expect your premises to be searched

The Serious Organised Crime and Police Act 2005 allows police, subject to the PACE procedure (see 34.6.2.1 in *McNae's*) for search warrants for journalistic material, to obtain a warrant to search all property occupied or controlled by the person named in the warrant and not merely specific premises.

But before issuing an all-premises warrant a judge must be satisfied that:

(1) there are reasonable grounds for believing that it is necessary to search premises occupied or controlled by the person in question which are not specified in the application, as well as those which are, in order to find the material in question; and
(2) it is not reasonably practicable to specify all the premises which he/she occupies or controls which might need to be searched.

Remember your rights!

Courts must allow media organisations access to all the police evidence when dealing with police requests for orders under PACE, the Supreme Court ruled in March 2014 *(R (on the application of British Sky Broadcasting Ltd) v The Commissioner of Police of the Metropolis* [2014] UKSC 17).

34.11 Other statutes

In addition to PACE, official secrets law (see *McNae's* ch.33) and counter terrorism law could affect journalists by placing them under a legal obligation to disclosure information including a source's identity. For counter-terrorism law, see 34.6.3 in *McNae's* and the online chapter 40 on www.mcnaes.com.

Other laws could place journalist under such legal obligation - for example, during an official investigation into fraud or 'insider' share dealings. These include:

- Section 2 of the Criminal Justice Act 1987, which empowers the director of the Serious Fraud Office (SFO) to summon anyone believed to have information relevant to an investigation. Anyone who fails to answer questions or give information faces a fine or up to six months in jail. There is no public interest defence for refusing to co-operate.
- The Financial Services and Markets Act 2000, as amended, which gives powers to financial regulators to demand information and documents.

34.12.1 Photos and footage of disorder

As explained in 34.12 in *McNae's*, journalists and media organisations, to maintain a reputation for neutrality may decide not to surrender voluntarily material which police request.
For example, untransmitted footage of the riots in London in August 2011 was handed to the police by BBC, ITN and Sky News only after police obtained production orders under PACE. PACE is outlined in 34.6 of *McNae's*. A judge might reject the application for a production order if, among other reasons, he/she does not consider it in the public interest to grant it.

Media organisations have repeatedly argued that it is not in the public interest for the police, by gaining - through production orders – access to the media's unpublished footage and photos. This 'public interest' argument is expressed by journalists and media organisations by citing their rights under Article 10 of the European Convention on Human Rights to gather news without interference by a state agency, such as the police. For example, in the case of the footage shot at Dale Farm – see the case study, below –media organisations argued that production orders are capable of discouraging or preventing journalists responsible for visual news coverage from carrying out such work. The argument is that if the perception takes hold among the public that journalists shooting footage and taking photos are working on behalf of the police, or are likely to co-operate with the police by supplying such material routinely to them, life could become very difficult for journalists on the ground. For example, it was argued that they might find it more difficult to obtain access to areas where demonstrations are taking place or to work in the vicinity of those who are prone to violence. Also, the media's argument includes that such a perception could increase the risk of violence towards camera operators, photographers or their equipment. In nearly every such case judges have ruled that the police's need – in the public interest - for evidence of rioting or other disorder outweighed the media's Article 10 rights, though the case described below was an exception.

Case study: In 2012 the High Court overturned a production order made by a judge at Chelmsford Crown court for broadcasters to hand over more than 100 hours of footage of

evictions from the Dale Farm travellers' site. The High Court said there were no reasonable grounds to believe that the footage included material likely to be of substantial value to the police investigation. The court added that applicants for such an order had to produce 'clear and compelling' evidence that it was necessary. In the judgment, Lord Justice Moses said a judge facing such an application by the police for media footage also had to exercise discretion in a manner compatible with Article 10, even if the conditions in PACE for having the material were satisfied, and added: 'First, the objective must be sufficiently important to justify the inhibition such orders inflict on the exercise of the fundamental right to disseminate information. Second, the means chosen to limit the right must be rational, fair and not arbitrary, and third, the means used must impair the right as little as is reasonably possible' *(R (on the application of BSkyB, the BBC, ITN, Hardcash productions Ltd and Jason Parkinson) v Chelmsford Crown Court* [2012] EWHC 1295 (Admin); [2012] 2 Cr App R 33; [2012] EMLR 30).

! Remember your rights

The Data Protection Act does not require journalists to disclose material which could help reveal a source's identity. For detail and a case study, see the Additional Material for ch. 28 on www.mcnaes.com.

Useful Websites

https://www.theguardian.com/world/2016/jul/12/snoopers-charter-could-endanger-journalists-and-sources-peers-warn

Coverage in *The Guardian* of House of Lords debate on the 2016 Act

https://ipco.org.uk/default.aspx

Website of Investigatory Powers Commissioner's Office which includes information about the Judicial Commissioners

https://www.gov.uk/government/publications/investigatory-powers-act-2016-codes-of-practice

Investigatory Powers Act codes of practice June 2018

https://www.gov.uk/government/publications/covert-surveillance-and-covert-human-intelligence-sources-codes-of-practice

Covert Surveillance and Property Interference Code of Practice August 2018
Covert Human Intelligence Sources Code of Practice August 2018