Extended material
Chapter 34: The journalists' sources and neutrality

RIPA - the powers the authorities have

Journalists using confidential sources to investigate crime or other wrongdoing, or who may themselves be accused of breaking the law because they are receiving leaked official information, should be aware that the Regulation of Investigatory Powers Act 2000 (RIPA) gives police and other agencies extensive power, in circumstances it defines, to intercept communications, gain records of telephone numbers dialled and of email traffic, and of the areas from which mobile phone calls are made, and to conduct surveillance, as explained below.

These powers are not designed specifically to target journalistic activity, but could target it. As the so-called 'Plebgate' episode demonstrated this sort of official interception or surveillance could lead to police or other agencies identifying journalists' confidential sources unless adequate steps are taken to protect them – see McNae's, 34.3.

Alan Rusbridger, former editor of *The Guardian*, warned at a conference in 2016: "The figures from 2015 show that 19 police forces have made 608 applications for communications data to find journalistic sources from 82 journalists in three years" (*Media Lawyer*, 21 June 2016).

There is also the possibility that non-official agencies can improperly access phone data.

See *McNae's*, 34.8, for other steps needed to protect confidential sources.

Interception

RIPA says that the Home Secretary can issue a warrant authorising interception (that is, disclosure of the contents of communications) after an application from specified officials of the police, security services, and HM Revenue and Customs, but must not do so unless he/she believes the warrant is necessary in the interests of national security, or to prevent or detect serious crime, or safeguard the UK's economic well-being, or to give effect to the provisions of any international mutual assistance agreement, and that the conduct authorised by the warrant is proportionate to the objective of the conduct. The Home Secretary must also consider whether the information could reasonably be obtained by other means.

Disclosing 'communications data'

The phrase 'communications data' in RIPA does not include the content of the communications, but - journalists should note - does include information such as telephone numbers dialled, the date and time of calls, the identities of people to whom emails are sent. The location of a person making calls on mobile or landline telephones can also be found.

The Act allows police, H M Revenue and Customs, the intelligence services, and any other 'public authority' specified by the Secretary of State to demand such information – for example, from phone companies - on the basis of authorisation by a designated person within that organisation. But a new legal safeguard means that a Crown court judge must approve any such 'production order' for a journalist's communications data, see *McNae's*, 34.3.2-34.3.3.

Communications data can be obtained in the interests of public safety; to protect public health; to assess or collect any tax, duty, levy, or other imposition, contribution, or charge payable to a government department; in an emergency, to prevent death or injury, or damage to someone's physical or mental health, or to mitigate such injury or damage; or for any purpose specified by order of the Secretary of State.

If the communications data is a journalist's, the person giving the authorisation ought to have regard to the need to respect freedom of expression, but there is no express statutory provision within the Act to do so.

Mobile phones betray location

A journalist who intends to meet a confidential source should not take his or her mobile phone to the meeting place if there is any prospect of official agencies trying to identify the source.

Some location data from each phone is automatically collected from cell masts by the phone's service provider, to route calls, and this data is stored. And the default setting of a phone may mean it is sending a GPS signal which betrays its exact location.

Mr Rusbridger warned that mobile phones such as the iPhone had location-plotting facilities which meant that the owner's movements could be tracked over weeks or months - and matched with a suspected source to prove a link or relationship (*Media Lawyer*, 21 June 2016).

Surveillance

As *McNae's* chapter 34 warns, a journalist may be put under surveillance by an official agency wanting to know who his or her sources are. Under RIPA surveillance can be 'directed' or 'intrusive'. 'Intrusive surveillance', for the purposes of the Act, is covert and involves use of a surveillance device, or the presence of a person, in residential premises or a private vehicle. Confusingly, any other surveillance is described as 'directed', no matter how intrusive it is.

Schedule 1 to the Act gives a lengthy list of public authorities whose designated representative can authorise directed (but not intrusive) surveillance. Authorisation for intrusive surveillance, which must be given by a designated person (for example, a chief constable), must be approved by a surveillance commissioner, a person who holds or who has held high judicial office.

The Home Secretary may authorise surveillance in intelligence and defence matters.

Investigation of electronic data protected by encryption

Powers in the Act mean that a person (including a journalist) may be required to disclose to official investigating agencies the encryption code of emails, or of other data, and could face a prison sentence for tipping anyone off that his/her emails are compromised.

Other statutes

In addition to RIPA, PACE and official secrets law – see *McNae's*, chapter 34 - various statutes could affect journalists by placing them under a legal obligation to disclose information including a source's identity - for example, to 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.
- Sections 62 and 63 of the Serious Organised Crime and Police Act 2005, which give the National Crime Agency, police, and H M Revenue and Customs powers to compel production of documents and demand information on specific issues. But journalistic documents and records held in confidence continue to be protected as the Act provides that no-one can be compelled to disclose 'excluded material'. This term is explained in *McNae's, 34.6.1.2*.
- The Financial Services and Markets Act 2000, as amended, which gives powers to financial regulators to demand information and documents.

Article 8 privacy rights may be engaged

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 April 2013.

A warrant to search a newspaper office was, in the circumstances, a violation of Article 8 and, because it 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, 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.

The applicant subsequently applied, unsuccessfully, to the domestic courts for an order cancelling the search warrant, arguing that the search of the newspaper's premises violated Article 8 of the Convention.

The fifth chamber of the Strasbourg court rejected the notion that Article 8 only protected individuals' homes, saying that the term 'home' 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 - had there 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.

Thus, the search and seizure were not proportionate and 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 – meaning the search was disproportionate and a breach of Article 10 as well.

- *McNae's* authors are grateful to Hugh Tomlinson QC and the Inforrm blog for their gracious 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.