JOURNALIST, TERRORIST OR COUNTER-TERRORIST?
THE PERILS OF INVESTIGATIVE JOURNALISM POST-9/11

by Clive WALKER, School of Law, University of Leeds, Leeds LS2 9JT, United Kingdom.

INTRODUCTION

Freedom of information and governmental transparency require champions. Lawyers and even some politicians may fondly believe that they are the self-appointed champions. However, journalists may have at least an equal claim to a leadership role. They may be viewed as unencumbered by the special interests of their client or their political party. More positively, journalists have a special public interest role to play in informing the public.

The European Court of Human Rights has been keen to underline the press role as champions of informing the public, including even in regard to the reporting of materials regarding terrorism, such as the speech of an extremist. In Castells v. Spain,1 it was suggested that:

“Freedom of the press affords the public one of the best means of discovering and forming an opinion of the ideas and attitudes of their political leaders. In particular, it gives politicians the opportunity to reflect and comment on the preoccupations of public opinion; it thus enables everyone to participate in the free political debate which is at the very core of the concept of a democratic society.”

The conferment of a special press role was extended in Jersild v. Denmark,2 where the European Court of Human Rights accepted that “Although formulated primarily with regard to the print media, these principles doubtless apply also to the audio-visual media”.

One may also find in the jurisprudence of the European Court of Human Rights more specific approbation of the role on investigative journalism through its attraction of an especially high

---

level of protection in principle, both against claims to the disclosure of sources\(^3\) and challenges by way of libel suit.\(^4\)

In pursuit of their role as champions of freedom of information and governmental transparency, journalists are avid customers of freedom of information legislation. The House of Commons Justice Committee in its report, *Post-legislative scrutiny of the Freedom of Information Act 2000*,\(^5\) was told by the Society of Editors that, “The Act has become an essential journalistic tool which has helped create a climate of genuine openness and transparency in British public life.”\(^6\)

This paper does not directly address the technicalities of freedom of information legislation as encountered by journalists. Instead, there is a broader theme but a narrower context. The focus is on investigations by journalists in which they seek to bring new information to the attention of the public but confined to the issue of terrorism. Attention was drawn to this theme in the United Kingdom by the case of David Miranda in 2013. He was detained as a suspected terrorist at Heathrow Airport for the possession of materials supplied from Edward Snowden, materials being transported from Russia to Brazil for journalistic purposes. This episode, which is considered later, is dramatized by title of this paper, “Journalist or Terrorist”. However, this paper addresses a wider issue than the precise circumstances of the Miranda case which is how journalism has been affected by the context of terrorism.

The threat of terrorism works in two ways against journalism. First, the stance of terrorists towards journalists seems to have become much more hostile. In recent times, journalists have become targets rather than witnesses or messengers. One early example of this trend was the killing of Daniel Pearl in Pakistan in 2002.\(^7\) More recent illustrations of the targeting of journalists involve the murder of *Charlie Hebdo* journalists in Paris on 7 January 2015\(^8\) and

---


killings by the Islamic State and its affiliates in Syria. Reasons for this growing hostility may include not only the vehemence of the rejection by Islamist groups of modernist cultures, but also, and paradoxically, their embrace of new media technologies. The internet affords several advantages to terrorists; compared to print media, it is harder to control and close down, it has better cross-jurisdictional reach, and it has lower running costs. Furthermore, the internet means that terrorists are no longer wholly reliant on the established (and often Western based) mass media to act as carriers and intermediaries, thereby allowing them to attain otherwise unattainable prominence, explicitness, and meaning to their violence. Thus, the internet now presents terrorists, whether mass movements or lone actors, with increased opportunities to propagate globally their own interpretations and messages, and so jihadi web and their online fans — “jihobbyists” — increasingly have greater recourse to mainstream social media platforms. Al-Qa’ida in the Arabian Peninsula’s online Inspire publication has been viewed as highly successful. Now, IS and their online supporters have proven themselves to be adept and prolific producers and disseminators of digital content. This growth of online content from terrorist groups and its potential attractiveness to, and

---


resonance with, discontented “digital natives” (young people who have grown up with the internet) have become causes of official apprehension throughout Europe17 and globally. Therefore, the United Nations Security Council Resolution 2178 of 24 September 2014 (“Addressing the growing issue of foreign terrorist fighters”), article 17, “urges Member States, in this context, to act cooperatively when taking national measures to prevent terrorists from exploiting technology, communications and resources, including audio and video, to incite support for terrorist acts, while respecting human rights and fundamental freedoms and in compliance with other obligations under international law”.

It is dangerous enough to be under attack from terrorism, but what this paper is concerned with is the growing attack from the state when it is countering terrorism. The core purpose of the paper is first to compile some evidence of this counter-terrorism threat to journalism. It is argued that a three-pronged attack emerges. First, there is the criminalization of journalistic activities by which the process of obtaining information and distilling it into news stories becomes depicted as a terrorist threat to the state. This first part of the paper considers the prime example of David Miranda. Second, there is the demand for information from the activities of journalism. In this way, journalism is coerced into serving state interests, even if contrary to the journalistic ethics on which the information was amassed. This second aspect may involve the voluntary trading of information through ongoing police-media relationships, but the interest of this paper lies in more coercive approaches. These will involve demands backed by legal sanctions, such as criminal offences or contempt of court. Third, and perhaps most insidious of all, there is a demand for proactive information-giving from the media to the security authorities. In the United Kingdom, there is again an element of criminal coercion through anti-terrorism laws which is not common elsewhere in the Western world. This imposed duty of the media to provide information proactively without demand has become broader and shriller.

Having explored these three areas of challenge, the next part of the paper will analyse why these trends are occurring. Several suggested causes are mentioned. Some relate to the nature of terrorism and counter-terrorism. Some relate to the nature of the media. The analysis will be followed by some conclusions and the appropriate reactions.

§ 1 – CRIMINALISATION OF JOURNALISTIC ACTIVITIES

The criminalisation of journalistic activities arises from the realization that investigative journalism can pose a threat to state security. By way of evidence of current attitudes, the Joint Services

17 See for example, See EU Counter-Terrorism Coordinator in consultation with the Commission services and the EEAS, Foreign Fighters and returnees (16002/14, Brussels, 2014) pp.2-3.
Publication 440, United Kingdom Ministry of Defence, a restricted security manual which was issued in 2001 and later revealed by Wikileaks, is instructive. It lists investigative journalists as a “non-traditional threat” to security whose activities are to be guarded against in the same way as foreign intelligence services and subversive or terrorist organizations. Thus:

“Government assets are under threat from a variety of sources beyond those traditionally regarded as hostile or otherwise of significance in terms of national security. The responsibility for providing advice to counter non-traditional threats will not always lie with the security staff and may often be provided by the appropriate Service, MOD or civil police agency. The main threats of this type are posed by investigative journalists, pressure groups, investigation agencies, criminal elements, disaffected staff, dishonest staff and computer hackers.”

This perception is not new. Various prominent prosecutions have been mounted against investigative journalists under official secrets legislation. Prominent examples in the modern era have included: R. v. Cairns, Aitken and Roberts in 1971, concerning a military assessment of the Biafran war; and R. v. Aubrey, Berry and Campbell in 1978, concerning army signals intelligence. In the case of The Guardian, in 2011, the Metropolitan Police began proceedings to force the newspaper to reveal how it obtained information that the mobile phone of a missing schoolgirl (Milly Dowler) had been hacked. However, the consent to prosecution of the Director of Public Prosecutions was not forthcoming.

The danger of the criminalization of journalists in connection with their reporting of terrorism lurks not only in the breadth of information which a government might view as useful to terrorism but also in what is counted as “terrorism”. Amongst the special offences of greatest threat to journalism in the United Kingdom include section 58 (possession of information useful to terrorism),

---

19 Ibid., para 0111.
20 Most were brought under the Official Secrets Act 1911, s. 2, which was repealed and replaced by the Official Secrets Act 1989. See Departmental Committee on Section 2 of the Official Secrets Act 1911, REPORT (Cmdn.5014, London, 1972); Home Office, REFORM OF SECTION 2 OF THE OFFICIAL SECRETS ACT 1911 (Cmd.7285, London, 1978); Home Office, REFORM OF SECTION 2 OF THE OFFICIAL SECRETS ACT 1911 (Cm.408, London, 1988)
section 58A (eliciting, publishing or communicating information about members of the security forces of a kind useful for terrorism such as by taking photographs), and the offence of attending training sites under section 8 of the Terrorism Act 2006.

The most prominent recent illustration is, as mentioned earlier, the case of David Miranda. Miranda was not charged with any offence, but the portrayal of him (and his colleagues) as suspected terrorists opened up special policing powers and raised the possibility of charges with special offences. In Miranda v. Secretary of State for the Home Department, the facts were that David Miranda was transporting computer materials (including files from the Government Communications Headquarters – “GCHQ”) supplied by Edward Snowden, a former contractor with the U.S. National Security Agency, to journalist Glenn Greenwald to assist ongoing disclosures in The Guardian about GCHQ and the NSA. The materials were seized during an examination and detention of Miranda while transiting through Heathrow Airport. The powers which were invoked were port and border control powers under Part V and Schedule 7 of the Terrorism Act 2000. Their purpose is to disrupt possible terrorist planning and logistics and also to gather intelligence. The controls also deter attacks on the travel facilities themselves. Examining officers (who are mainly police officers) may question a person under Schedule 7, paragraph 1, for the purpose of determining whether he appears to be a “terrorist” within the Terrorism Act 2000, section 40(1)(b).

Reflecting the “all-risks” nature of these powers, examining officers may exercise their powers whether or not they have suspicion against any individual (paragraph 2). In this way, the “copper’s nose” may guide application. Some interventions will be based on intelligence perhaps related to destination, behavioural signals, or on documentary irregularities. However, the use of examinations for extraneous purposes, such as to build the case for the issuance of an executive order, is not permitted, as sustained in CC v. Commissioner of Police for the Metropolis. At the same time, that case confirms: that the basis for intervention can be intuition; that the powers can be applied against someone already suspect in order to determine details of involvement; and that examinations can

26 See Sch.7, paras.1(3), 2(2); Immigration Rules 2003, rr.47–49.
29 See C. Walker, Neighbor terrorism and the all-risks policing of terrorism (2009), 3 JOURNAL OF NATIONAL SECURITY LAW & POLICY 121.
continue even if initial indications of terrorism are negative.\textsuperscript{33} A requirement of reasonable suspicion would, it is claimed, compromise police capability to detect terrorism\textsuperscript{34} such as where a person is involved “unknowingly” or is of interest based on their destination.\textsuperscript{35} Reasonable suspicion requirements might also encourage the use of “clean skins”, alert suspects to surveillance, and prevent the examination of travel companions.\textsuperscript{36} To allay some these concerns, an accompany Code of Practice issues an admonition not to discriminate or to select based on ethnic characteristics\textsuperscript{37} and seeks to focus selection based upon: “Known and suspected sources of terrorism; Individuals or groups whose current or past involvement in acts or threats of terrorism is known or suspected, and supporters or sponsors of such activity who are known or suspected; Any information on the origins and/or location of terrorist groups; Possible current, emerging and future terrorist activity; The means of travel (and documentation) that a group or individuals involved in terrorist activity could use; Emerging local trends or patterns of travel through specific ports or in the wider vicinity that may be linked to terrorist activity; and/or Observation of an individual’s behaviour”\textsuperscript{38}.

In the case of Miranda, the initial view of the Security Service (MI5), which issued a “Port Circulation Sheet” to the police Counter Terrorism Command regarding Miranda, was that Schedule 7 was “not applicable”.\textsuperscript{39} These doubts were not conveyed to the examining officers on the ground. However, a third round of deliberations by the security agents concluded that Miranda was concerned in terrorism because his mission sought to influence the government by promoting a political or ideological cause under the Terrorism Act 2000, section 1(1)(b) and (c).\textsuperscript{40} An alternative explanation, which denies the applicability of Schedule 7 and claims that the mission was one of revealing interesting facts to sell newspapers, was not proffered as such, and, instead, Greenwald claimed in the subsequent litigation the purpose of “responsible journalism” in the public interest,\textsuperscript{41} an asserted privilege dismissed on the basis that journalists have no constitutional responsibility.\textsuperscript{42} By comparison, a more convincing claim to a purely journalistic
mission was sustained in *R v. Murney*.

Here the collection of information about policing in Newry by an officer of *éirígí* (a socialist republican political party in Ireland) was not an offence under the Terrorism Act 2000, section 58A (eliciting, publishing or communicating information about members of the security forces which is of a kind likely to be useful for terrorism); while photographs of police activity could assist terrorism, proof of a reasonable cause — public concern about police abuses — was sustained. As for potential impact under the Terrorism Act 2000, section 1(2)(c) and (d), it was sufficient that the examining officers contemplated that disclosure of data to a hostile state (Russia) or to terrorists might imperil the identities of secret agents or the methods used for electronic surveillance of terrorists.

Thus, the material was placed in the realms of terrorism and not just official secrecy.

The formulation of “terrorism” in the mind of the examining officer did not require any specific offence to be formulated, nor must *mens rea* (beyond the “design” and “purpose” detectable from the mission) be established on the part of the traveller since there could be interest either in material being transported or in the traveller.

Nevertheless, the power must be exercised on “some reasoned basis, proportionately … and in good faith”. There was no need to conclude that Miranda was a person falling within section 40(1)(b) prior to the stop.

Nor did his express targeting exclude the exercise of Schedule 7; as stated in *CC v. Commissioner of Police of the Metropolis*, “the language of s.40(1)(b) is wide enough to allow for examination not only of whether he appears to be a terrorist but also of the way in which or the act by which he so appears.”

There was a compelling and proportionate interest to seize the data, especially as the court denied the status of “journalistic materials” within Article 10, albeit on the dubious basis that they had been stolen.

The Independent Reviewer of Terrorism Legislation (David Anderson) commented that the High Court had endorsed so a wide ambit for the term “terrorism” that journalists and newspapers could potentially become subject to special criminal offences, could be proscribed (banned), could be designated under terrorist asset-freezing legislation, and could be subjected to executive restraint orders.

At the same time, the potential must be seen in the context of requirements of proportionality and respect for
rights to free speech, so that Law Justice Laws made clear that “There is no suggestion that media reporting on terrorism ought per se to be considered equivalent to assisting terrorists”\textsuperscript{52} 

As well as being stopped for examination, the traveller may also be searched under paragraph 8 by an examining officer (or a person authorized under paragraph 10).\textsuperscript{53} Property may be seized for investigation for seven days under paragraph 11. An increasingly common seizure scenario has involved the capture of data from laptops, data devices, and mobile phones. The practice has been to return the hardware within seven days but to keep the copied data in accordance with the guidance in the Management of Police Information (“MoPI”),\textsuperscript{54} which suggests a six-year retention period.\textsuperscript{55} Seizure of data, which was being transported for journalistic purposes, was at the heart of a further hearing in \textit{R (Miranda) v. Secretary of State for the Home Department}.\textsuperscript{56} An interim hearing was held about the seized computer data. It was held that inspection may take place for the purposes of securing national security or for the investigation of terrorism.\textsuperscript{57} There was no exemption for journalistic materials. Once the material is obtained under Schedule 7, it can be transferred to the security authorities under section 19 of the Counter Terrorism Act 2008. The data was transferred and retained even though Miranda was allowed to depart, and no further legal action has ensued either in relation to the data or Miranda (whose criminal mens rea might be affected by the heavy encryption of the data). The High Court referred to the data being “stolen”,\textsuperscript{58} but Snowden held copied information,\textsuperscript{59} and the hardware possessed by Miranda was not stolen. Consequently, no evident legal basis for police retention emerged to override paragraph 11.\textsuperscript{60} Reflecting the need to keep up to date with technological developments,\textsuperscript{61} as highlighted in the Miranda case, later legislation, the Anti-social Behaviour, Crime and Policing Act 2014, Schedule 9, paragraph 4 inserted paragraph 11A into

\begin{itemize}
  \item \textsuperscript{52} \textit{David Miranda v. The Secretary of State for the Home Department and The Commissioner of the Police of the Metropolis} [2014] EWHC 255 [35]
  \item \textsuperscript{53} These provisions were reformed by the Anti-Social Behaviour, Crime and Policing Act 2014, Sch.9, following the Home Office, \textit{REVIEW OF THE OPERATION OF SCHEDULE 7: A PUBLIC CONSULTATION} (London, 2012).
  \item \textsuperscript{56} [2013] EWHC 2609 (Admin).
  \item \textsuperscript{57} Ibid., para 32.
  \item \textsuperscript{58} \textit{Miranda v. Secretary of State for the Home Department} [2014] EWHC 225, para. 8.
  \item \textsuperscript{59} \textit{See Oxford v. Mass} (1979) 68 Cr App Rep 183.
  \item \textsuperscript{61} Hansard (House of Commons) Public Bill Committee col.454 (9 July 2013), Damian Green.
\end{itemize}
Schedule 7. It grants an express power for police constables only to make and retain copies of anything obtained from searches under paragraph 5, 8, or 9. Copies may be retained for as long as is necessary for investigative purposes or for use as evidence in criminal or deportation proceedings. However, retention is subject to the Data Protection Act 1998 and the MoPI guidance. Suggestions that these powers (and other search powers in Schedule 7) should be exercisable on reasonable suspicion and that legally privileged and special procedure (including journalistic) material should be exempted were rejected during passage through Parliament.

The Home Office is confident that the port controls are compliant with the European Convention on Human Rights following the changes in the Anti-social Behaviour, Crime and Policing Act 2014, having previously received assurances to that effect in the cases of Gillan and Quinton v. United Kingdom, Beghal v. DPP, and Miranda. Intrusions on liberty probably fall within the exception for a stated legal “obligation” under Article 5(1)(b), with particular indulgence being shown for intrusions at borders. This verdict was reached by the European Commission of Human Rights in regard to travellers to and from both parts of Ireland in McVeigh and in Harkin, X, Lyttle, Gillen, and McCann v. United Kingdom. Next, in Gillan and Quinton v. United Kingdom, the European Court of Human Rights viewed the exercise of search powers at ports and airports as being excused by consent under Article 8. A wide catalogue of rights was considered in Beghal v. DPP. As the wife of a convicted terrorist, Djamel Beghal, the cause of her examination was evident under Article 5. Her Article 8 complaint was not sustained because the surveillance of airport travellers is intrinsic to contemporary travel. An Article 6 complaint was also dismissed since criminal proceedings were not

62 Hansard (House of Commons) Public Bill Committee col.456 (9 July 2013), Damian Green.
64 Hansard (House of Lords) vol.750, col.810 (11 December 2013).
69 See Gillan and Quinton v. United Kingdom, App No.4158/05, 12 January 2010, para. 64; Gabramanov v. Azerbaijan, App. No.26291/06, 7 November 2013.
72 A further challenge is pending in Malik v. United Kingdom, App. No.32968/11.
73 [2013] EWHC 2573.
contemplated and certainly none based on her answers. The *Miranda* case underlines that the journalistic materials under Article 10 may yet prove problematic, given that no express recognition is given to special procedure materials or legal privilege. Assessing the application of port controls to journalism in the *Miranda* case, it must be concluded that the special laws were rather strained, as recognised initially by the Security Service and the police. A power to examine and search for materials the possession of which is contrary to United Kingdom law would offer a more suitable legal vehicle and a wider power of intervention than rules as to import and export (such as weapons) or as to customs dues.74 Materials held in breach of official secrets laws could thereby be protected. A less ambitious legal reform would be to insert within the port controls recognition of journalistic privilege, though, as already indicated, this proposal was specifically rejected by Parliament.

§ 2 – Demand for Information

Cooperation between police and media is ingrained in both low and high policing.75 There are two common modes of engagement. The principal mode of relationship is managerial. In this mode, the police, albeit that they are powerful initiators in criminal justice and can wield coercive powers, are concerned with news management - how information is released and understood through negotiation and interaction. Underlying this approach is a high degree of cooperation and mutual reliance between police and media, as well as recognition by the police of the independence and important roles of the media. As a consequence, many previous researchers have found that there is often a stable and productive relationship between the police and crime reporters.76 Thus, there is “a sense of dependency between police and members of the media, uneasy


Though this may be at times.\textsuperscript{77} While the police may sometimes seek to manipulate media coverage of their image and work,\textsuperscript{78} at the same time the police depend on the media for the regular conveyance of messages to the public and also at times utilise the media as an investigative resource.\textsuperscript{79} In turn, journalists depend upon the police for primary information. It is difficult to be conclusive about which side acts as primary information-gatekeepers. Without hard law to regulate self-serving relationships, temptations to give and take may arise and have indeed been at the heart of inquiries into press conduct in relation to telephone tapping and other breaches of privacy in the United Kingdom in recent years.\textsuperscript{80} One major impact was the closure of the \textit{News of the World} newspaper in 2011. Journalists have also been convicted of breaches of the Data Protection Act 1998 and the Regulation of Investigatory Powers Act 2000,\textsuperscript{81} while their police collaborators have also been convicted of corruption.\textsuperscript{82}

The second mode for police-media relations is coercive. In certain circumstances, the police can coerce the media into action or inaction through the application of legal powers. One such application might involve the use of the media as surrogate investigators and information sources. This mode of relationship is not common in the United Kingdom. Freedom of the press is accorded a high value in United Kingdom constitutional law, as evidenced by the special protection for “freedom of expression” in section 12 of the Human Rights Act 1998, building upon the European Convention on Human Rights and Fundamental Freedoms of 1950, Article 10. Nevertheless, the coercive demand for information may arise under threat of legal powers or under the actual invocation of legal powers. In either case, there is a strong element of coercion and threat.

This modality arose in the \textit{Miranda} case. On 20 July 2013, even before the Heathrow Airport incident (which occurred on 18


\textsuperscript{78} House of Commons Home Affairs Committee, \textit{POLICE AND THE MEDIA} (2008-09 HC 75), para. 29.

\textsuperscript{79} M. Innes, \textit{The media as an investigative resource in police murder enquiries}, (1999) 39 \textit{British Journal of Criminology} 269.


\textsuperscript{81} Examples include Clive Goodman (2007); and Dan Evans, Graham Johnson, Ian Edmondson, Neville Thurlbeck, Greg Miskiw, James Weatherup, and Andy Coulson (2014).

\textsuperscript{82} See Alan King and Paul Marshall (2005); April Casburn 2013.
August 2013) but revealed after that event, The Guardian disclosed that GCHQ had forced the newspaper to destroy Snowden-related documents or face legal action. They were informed by the authorities, “You’ve had your fun. Now we want the stuff back.”

The materials were held in the basement of the newspaper’s offices. In the presence of GCHQ technicians, a senior editor and a Guardian computer expert used angle grinders and drills to “pulverise the hard drives and memory chips on which the encrypted files had been stored”. It was appreciated that the destruction was a show of force, because all parties knew that other copies of the data were held elsewhere – in Russia, the U.S., Brazil, and China. But the authorities wanted this destruction to take place to ensure the security of sensitive data within the United Kingdom at least. The newspaper complied, fearing either a civil injunction or criminal proceedings under the Official Secrets Act. In the event, they chose to destroy the documents rather than hand them over so as to avoid any extraneous markings and also to avoid revealing the extent of their catalogue.

If the obliteration of journalistic materials under threat of legal action does not sound drastic enough, more legalistic processes can be actually invoked. Again, this approach is not a novel, and legal activities in connection with infractions of the Official Secrets Acts have already been noted. But demands for information are becoming firmly attached to counter terrorism operations, as revealed in two ways.

The first aspect concerns the use of special search powers in Schedule 5 of the Terrorism Act 2000. Schedule 5 offers variants upon Schedule 1 of the mainstream policing legislation (namely, the Police and Criminal Evidence Act 1984 – “PACE”). The main differences are the triggering criteria, which relate to “terrorist investigations” rather than to specified offences, and the more extensive powers so triggered. The catalogue includes powers to enter premises, to search the premises or any person found there, and to seize and retain any relevant material. By Schedule 5, paragraph 1(1): “A constable may apply to a justice of the peace for the issue of a warrant under this paragraph for the purposes of a terrorist investigation.” The premises to be targeted may be particular (for a “specific premises warrant”) or, following amendment by the Terrorism Act 2006, section 26, they may comprise any or sets of premises occupied or controlled by a person specified in the application (an “all premises warrant”).

“Excepted material” may not be the subject of an application, and that term is defined in paragraph 4 by reference to corresponding

PACE exceptions. These comprise “excluded material” (under section 11 of PACE, which includes journalistic material which a person holds in confidence and which consists of documents or of records other than documents), “special procedure material” (under section 14 of PACE, which includes all other journalistic material, other than excluded material) and “items subject to legal privilege” (under section 10 of PACE). Journalistic material is defined in section 13 of PACE:

“(1) Subject to subsection (2) below, in this Act ‘journalistic material’ means material acquired or created for the purposes of journalism.

(2) Material is only journalistic material for the purposes of this Act if it is in the possession of a person who acquired or created it for the purposes of journalism.

(3) A person who receives material from someone who intends that the recipient shall use it for the purposes of journalism is to be taken to have acquired it for those purposes.”

In the light of these exceptions, the Terrorism Act 2000 search powers have not been recorded as being used against journalists, but an attempt to secure information from The Guardian and The Observer about possible breaches of official secrets legislation was made in R v. Central Criminal Court, ex parte Bright. A decade and a half ago, the judgment emphasized the value of journalism:

“... Premises are not to be entered by the forces of authority or the State to deter or diminish, inhibit or stifle the exercise of an individual’s right to free speech or the press of its freedom to investigate and inform... Inconvenient or embarrassing revelations, whether for the Security Services, or for public authorities, should not be suppressed.”

More threatening is the next investigative power, under Schedule 5, paragraph 5, which deals with the production of, or access to, (rather than the physical search for) “excluded” and “special procedure” materials. By paragraph 8, only legally privileged material is wholly exempted from the clutches of paragraph 5. By paragraph 5(1), a constable may apply to a circuit judge for a production order to access excluded or special procedure material (including, under paragraph 7, material coming into existence within 28 days) for the purposes of a terrorist investigation. There is no requirement that notice be given to the possessor of the materials or that the material must be potential “evidence” for a court case. If granted, the order may require under paragraph 5(3) a specified person normally within seven days: (a) to produce to a constable within a specified period for seizure and retention any relevant material; (b) to give a constable access to relevant material within a specified period; and (c) to state to the best of his

---

86 See R v. Crown Court at Bristol, ex p Bristol Press and Picture Agency Ltd (1986) 85 Cr App Rep 190, DC (press photographs of riots were special procedure material).
87 [2001] 1 W.L.R. 662 (DC).
88 Ibid., paras. 97, 98.
knowledge and belief the location of relevant material if it is not in, and will not come into, his possession, custody, or power within the period specified under (a) or (b). An order may also require any other person who appears to the judge to be entitled to grant entry to the premises to allow entry and access. The circuit judge may grant an order if “satisfied” of two criteria in paragraph 6. The first condition relates to the relevance to the purposes of a terrorist investigation as well as the need for “reasonable grounds for believing that the material is likely to be of substantial value”. The second condition demands reasonable grounds for believing that it is in the public interest that the material should be produced. Under paragraph 10, the order is treated as if it were an order of the Crown Court and can be enforced by contempt of court powers. Much of the consequent litigation has related to journalistic materials. In R v. Middlesex Guildhall Crown Court, ex parte Salinger, the police sought from the prominent U.S. journalist, Pierre Salinger, and his employers records of interviews conducted in Libya with the two prime suspects of the Lockerbie bombing in 1988. On the initial ex parte application, the High Court held that the police should provide to the judge a written statement of the material evidence, including the nature of the available information subject to secrecy and sensitivity, and the applicant police officer should appear before the judge to provide oral evidence. The judge could then decide on the grant of the order and also on what information might be served on the recipients. In turn, the recipients will rarely be notified until the service of the order, when they are entitled to be given, preferably in writing, as much information as could properly be provided as to the grounds for the order but it would rarely be appropriate or necessary for disclosure of the source or details. Their subsequent application to discharge or vary should be made to the same judge with the same police officer who gave oral evidence being present. On this application, the judge can reconsider the order afresh on its merits, and there is no onus on the recipient to satisfy the judge that the order was wrongly made. It was later revealed that ABC News had agreed to comply because the order did not require the disclosure of confidential sources. Journalistic material was again investigated in 1991 when Box Productions compiled a television programme, broadcast by Channel 4, which alleged collusion between members of the Royal Ulster Constabulary and Loyalist terrorists which was presided over by a secret committee of prominent people. The police sought the production of documents connected with the programme. A

90 See also In re request from the United Kingdom (2013) 718 F 3d 13.
91 [1993] QB 564.
92 See further Re Morris [2003] NICC 11. But appearance might be allowed in difficult and complex cases involving the media: para. 35.
redacted dossier of material was handed over, but it was claimed that further sensitive material had either been destroyed or removed from the jurisdiction and that the only person who knew the whereabouts of the material was a researcher employed by Box Productions. The judge then directed that the material sent abroad should be brought back and produced to the police. The respondents refused to comply. The Divisional Court, which could not review the judge’s order, imposed a fine of £75,000 for contempt.

In Re Moloney’s Application,95 the Northern Ireland editor of the Sunday Tribune newspaper was required to produce notes of an interview with William Stobie, who was later accused of the murder of lawyer Patrick Finucane.96 Quashing the Recorder’s order, the High Court stated:

“… the police have in our view to show something more than a possibility that the material will be of some use. They must establish that there are reasonable grounds for believing that the material is likely to be of substantial value to the investigation.”

In Re Jordan,98 the police sought materials from a BBC Panorama programme, Gangsters at War, which transmitted an announcement by a masked man on behalf of the Ulster Freedom Fighters. He was identified through voice analysis as Dennis Cunningham.99 Any arguments about the chilling effect of disclosure on the ability to carry out investigative journalism were outweighed in the view of the Crown Court in Belfast by “the unmasking of terrorists and bringing them to justice”.100 By contrast, the BBC escaped compulsory disclosure by the Belfast Recorders’ Court of unbroadcast film of a Republican parade in Londonderry in 2011 in which a masked man read out a speech on behalf of the Real IRA.101 The police’s claim that the extra footage would aid identification was rejected under Schedule 5, paragraph 5, because no “substantial value” had been established by the police, though the court made clear that if the police had met the standard of proof, then the public interest would have outweighed claims by the media of increased risks in news-gathering.

In Malik v. Manchester Crown Court,102 a production order was granted in relation to a book manuscript written about Hassan Butt, entitled, Leaving Al-Qaeda. The police believed materials

100 [2003] NICC 1, para 21 per Judge Hart.
possessed by Malik, who helped to write the book, might disclose evidence of crimes by Butt. It was held that “likely” under paragraph 6(2)(b) demanded a high standard – “probable”; but “substantial value” required only a value more than minimal.\(^{103}\) Being “satisfied” required a firm belief rather than a suspicion.\(^{104}\) On review, the grant of the order was upheld, though the terms were altered. The High Court indicated that a court could of its own motion appoint a special advocate to appear at the \textit{ex parte} hearing or on an application for variation or discharge, but only in exceptional cases.\(^{105}\)

In \textit{Re Galloway}, the Police Service of Northern Ireland sought records and materials from the Northern Editor of the \textit{Sunday Tribune} newspaper relating to claims of responsibility for the murders by Republican dissidents of two soldiers in 2009.\(^{106}\) The application was refused. The Court endorsed the approach that the public interest in the investigation and prosecution of serious crime is important, so the level of proof of overriding interests must attain a very high threshold of a substantial risk — in this case the threat to the right to life (Article 2 of the Convention) of the journalist and her family. That standard was met by the journalist. Two issues not yet adequately litigated are, first whether compliance with the production order might involve forcible self-incrimination contrary to Article 6 of the European Convention on Human Rights. It was indicated in \textit{R v. Central Criminal Court, ex parte Bright}\(^{107}\) that the statutory powers of production override the right against self-incrimination.

The production of physical materials with an existence independent of the will of the defendant has been treated as distinct from demanding information from the knowledge of the defendant.\(^{109}\) The second factor to be considered is the impact of section 12(4) of the Human Rights Act 1998, which requires “particular regard” for the importance of freedom of expression before any order is granted.

Should a production order under paragraph 5 be viewed as inappropriate for the purposes of the investigation, then under paragraph 11, a constable may apply to a circuit judge (or in Northern Ireland, a Crown Court judge) for the issuance of a

\(^{103}\) \textit{Ibid.}, para 36.
\(^{104}\) \textit{Ibid.}, para 37.
\(^{105}\) \textit{Ibid.}, para 99.
\(^{107}\) [2001] 1 W.L.R. 662 (DC).
\(^{108}\) \textit{Beghal v. DPP} [2013] EWHC 2573 (Admin), paras.127-129. Appeal to the UK Supreme Court is pending.
warrant to permit entry, search, and seizure. This variant procedure may be selected where, under paragraph 12, a circuit judge is satisfied that a production order has not been complied with or where satisfied that there are reasonable grounds for believing there is present material likely to be of substantial value but that it is not appropriate to proceed by way of production order (perhaps because it would tip off a potential collaborator).

Another type of investigative power is ancillary to the foregoing. By Schedule 5, paragraph 13, a constable may apply to a circuit judge (or in Northern Ireland, a Crown Court judge) for an order requiring any person specified in the order to provide an explanation of any material seized, produced, or made available under paragraphs 1, 5, or 11.110 There is no equivalent to this invasive power in PACE 1984. There is no immunity against revealing information concerning other excepted materials. It is an offence under paragraph 14 knowingly or recklessly to make a false or misleading statement. By paragraph 13(4)(b), and in deference to Article 6, a statement in response to a requirement imposed by an order under this paragraph may be used in evidence against the maker only on a prosecution for an offence under paragraph 14 but not for other offences.111 There is no recorded use against a journalist.

The increasing usage of Schedule 5 reveals an official willingness to treat journalism as an available resource for the provision of journalistic information in pursuit of criminal justice purposes but without much emphasis (beyond that stated in ex parte Bright in 2001) for other public interests such as a free and fearless press. The relative success of the tactic seems to have emboldened the police, especially in Northern Ireland, and so this second tactic of confrontation of journalism is now being rolled out on a global scale. This new front has become more feasible after 9/11, when the tendency to treat terrorism cases as “political offences” and therefore not subject to international comity has tended to fall away, especially in the case of the U.S. authorities.112 The point is illustrated by litigation around the Boston College tapes.113

The “Belfast Project” began in 2001 as an oral history of the Northern Ireland Troubles. It was directed by journalist Ed Moloney, with the fieldwork being conducted by recorded by Wilson McArthur (for Loyalists) and Anthony McIntyre (for Republicans). The collection was to form a repository in the Burns Library at Boston College, thereby benefiting from full U.S. First Amendment rights and a degree of distance (so it was thought)

from the prying eyes of the British authorities. A key objective was to capture the views of live participants as a research resource and also part of the eventual process of transitional justice through account-giving. Various former loyalist and republican paramilitaries gave candid interviews that chronicled their involvement in the Troubles. They were promised that the recordings and transcripts would only be made public after their deaths. Amongst those interviewed were David Ervine of the Progressive Unionist Party, and the former IRA commander Brendan Hughes (who died in 2007 and 2008 respectively), and some details were revealed in a book by Ed Moloney,114 and a television documentary broadcast by Raidió Teilifís Eireann in 2010.115 It was probably naïve, arrogant, or both to suppose that the authorities would look the other way. Accordingly, the Police Service of Northern Ireland (“PSNI”) took action, after hearing claims in the published statements of Hughes that the Sinn Féin leader, Gerry Adams, had been overall commander of the IRA’s Belfast brigade and that he had been involved in a unit responsible for the “Disappeared” - those who were kidnapped, murdered and secretly buried by the IRA.116 Though denied by Adams, another prominent Republican participant in the “Belfast Project”, Dolours Price, who died in 2013, also gave information about her involvement in driving one of the “Disappeared”, Jean McConville to the place where she was murdered by the IRA in 1972.117

In March 2011, the PSNI began a legal bid in the U.S. to gain access to the interviews held by Boston College. Its investigation took the form of a request to the U.S. Department of Justice to initiate Mutual Legal Assistance Treaty proceedings by issuing a sealed subpoena for all materials relating to two interviews in the archive, those of Brendan Hughes and Dolours Price.118 Boston College sought to quash the subpoena.119 In August, 2011, a second subpoena was served seeking “any and all interviews containing information about the abduction and death of Mrs. Jean McConville.”120 This was also opposed by the Belfast Project, including on the political argument that the Attorney General should take cognisance of solemn promises made by the U.K. Government to the U.S. Senate that it would not reopen issues

114 Voices from the Grave: Two Men’s War in Ireland (Faber & Faber, London, 2011).
117 In August 2003, her remains were found by chance at Shelling Hill beach in County Louth. The IRA admitted her killing in 1999.
119 Ibid.
addressed in the Belfast Agreement, or [ ] impede any further efforts to resolve the conflict in Northern Ireland.[121]

In December, 2011, Judge William G. Young recognised that “subpoenae targeting confidential academic information deserve heightened scrutiny” but still ruled against both Boston College’s motions to quash the subpoenas and Moloney and McIntyre’s motion to intervene.[122] His proposal was to review the archives in camera, but this exercise was stayed pending an appeal to the U.S. Court of Appeals.[123] The First Circuit Court of Appeals gave judgment on the first subpoena on 6 July 2013, upholding Judge Young’s ruling.[124] Any First Amendment challenge was rejected on grounds that there were no private rights under these international law arrangements and there was no judicial review of actions under a treaty. A stay was granted by the U.S. Supreme Court,[125] but certiorari was denied in 2013.[126] The First Circuit Court of Appeals ruled on Boston College’s appeal and motions on 31 May 2013. The Court was critical of the breadth of the application and reduced the amount of material to be handed over from 85 interviews (out of 176 relevant interviews in total) to segments of 11 interviews.[127] But, at the same time, it crucially found that a promise of confidentiality by a researcher did not create a First Amendment bar.[128] The U.S. Attorney’s application for a rehearing was denied.[129]

In 2015, arrangements were made for sealed tapes to be sent to the Royal Courts of Justice in Belfast. At least three legal consequences have ensued. First, Richard O’Rawe has threatened to sue Boston College after it handed over parts of his interviews. He claims breach of contract:[130]

> “Mr. O’Rawe told of his career in the Provos to Boston College researchers on strict conditions contained in a ‘donor contract’ with the college. It stated that ‘access to the tapes and transcripts shall be restricted until after my death except in those cases where

---


123 https://bostoncollegesubpoena.wordpress.com/court-documents/plaintiff-appellants-brief/;


126 Moloney v. United States, 133 S. Ct. 1796, 185 L. Ed. 2d 856 (U.S., 2013).


128 Ibid., p.20.

129 https://bostoncollegesubpoena.wordpress.com/2013/09/05/first-circuit-ruling-on-us-attorney-petition-for-rehearing-denied/.

I have provided prior written approval’. However, the contract didn’t specify that the secrecy of the archive was limited under American law.”

Second, and even before the tapes had arrived, the police arrested Gerry Adams in May 2014 regarding his alleged role in the disappearance of Jean McConville. Adams was released without charge, and the then PSNI Chief Constable, Matt Baggott, rejected “claim there were ‘dark’ elements opposed to the peace process behind his detention”.

Third, and with the tapes now arriving on the doorstep of the United Kingdom jurisdiction, a number of interviewees are no doubt feeling distinctly uncomfortable. One such interviewee is Winston Rea, who was a member of the Red Hand Commando and who had provided testimony to the Belfast Project. Rea brought legal proceedings in Belfast to stop police from listening to the tapes. His counsel argued that prosecuting authorities were acting on a hunch rather than any firm knowledge that the tapes contain information relevant to any investigation and that the operative legislation, section 7(5) of the Crime (International Cooperation) Act 2003, breached Rea’s right to privacy under the European Convention on Human Rights, article 8. After the application was rejected in the High Court, the PSNI officers travelled to Boston for the purpose of taking possession of the tapes. On 27 February 2015, the Northern Ireland Court of Appeal rejected the appeal.

The DPP argued that the standard to be established was simply that the evidence should be “for use” in the proceedings or investigation rather than that it must be of “substantial value”. Given that the legal test applied by the USA in such cases was that of “probable cause”, the U.S. Court of Appeals decision showed that sufficient grounds were made out for the material to be subpoenaed. The DPP also argued that there was a duty to protect life under Article 2 of the European Convention on Human Rights to investigate murder in the interests of victims and the general public. Lord Justice Coghlin accepted that the material could properly be subpoenaed in connection with the investigation stage and that, as a consequence the PSNI do not have to identify specific aspects of the recordings which are relevant to the offences being investigated other than they purport to be an account of terrorist activities carried out by the Red Hand Commando of which the PSNI hold prior information, as noted in the letter of request to the USA authorities, indicating that Rea was an active member.

The standard specified in the 2003 Act for the grounds upon which the evidence is considered to be relevant for the purpose of a request for mutual assistance is that it is for “use in the proceedings or investigation”. Such evidence could not be of use if it was irrelevant but that was very far from reading into the

---


2003 Act any particular standard of relevance. Finally, any infringement of privacy would be covered by the exceptions in Article 8(2) to the European Convention on Human Rights. Though the judgment was decisively in their favour, before the PSNI could take away the tapes, the court ordered on that the material remained sealed pending an appeal to the United Kingdom Supreme Court.

In conclusion, this second round of intrusions into journalistic activities in order to support police and prosecution activities do again have the tendencies to downplay the wider public interest attributes of journalism and also produce a chilling effect on the journalists and their sources. The only silver lining compared to the first round of intrusions (and the third round to follow) is that the courts tend to be heavily involved in the supervision of these interventions. As a result, while savings for journalistic purposes are often absent from the operative laws, the judges are alert to the issues under articles 8 and 10 of the European Convention on Human Rights, though, as shown in the Boston Project cases, its standards are relatively weak, albeit that apparently stronger U.S. standards on free speech did not make much difference.

§ 3 – DUTY TO INFORM PROACTIVELY

The foregoing mode of imposition upon journalism in the interests of counter terrorism demands action at the behest of the police. This third mode of imposition seeks to bypass police initiative. After all, why should journalists wait for a call if their information can save lives and if the police are unaware who possesses juicy information in order to make a request? Better still to confer a general legal duty on everyone to inform without asking. Such a general duty would have particular purchase on journalism by recognising the forensic abilities of some journalists to obtain and analyse information which may sometimes exceed police capabilities in two ways. First, they may be able to carry out investigations not permissible in the case of the police because of threshold requirements as to action or limitations on investigative techniques. Second, journalistic activity may be unencumbered by the finances of the police in an age of austerity.133 So, the objective under this third heading is to make journalists duty-bound to serve up information about terrorism and not simply potential resources for search warrants or other forms of police-initiated investigation. The media must therefore turn themselves into self-tasking policing bodies.

This insidious duty has been conferred by the Terrorism Act 2000, section 38B.134 The offence is committed under section 38B(2) if a


134 See C. Walker, Conscripting the public in terrorism policing: towards safer communities or a police state? [2010] CRIMINAL LAW REVIEW 441; C. Walker, THE ANTI-
person, without reasonable excuse, fails to disclose information falling within section 38B(1), which is information which he knows or believes might be of material assistance in preventing the commission by another person of an act of terrorism, or in securing the apprehension, prosecution, or conviction of another person, in the United Kingdom, for an offence involving the commission, preparation, or instigation of an act of terrorism. This special duty has existed in various guises since 1976, while in Northern Ireland it is also an offence under section 5 in the Criminal Law Act (Northern Ireland) 1967 to fail to give information known or believed likely to secure, or to be of material assistance in securing, the apprehension, prosecution or conviction of any person for an arrestable offence which has been committed. Section 38B is different in that the information must relate to “terrorism” rather than an “arrestable offence” and may concern future as well as past activities. Nevertheless, the considerable overlap between section 38B and section 5(1) convinced the Baker Report to propose the repeal of section 5(1) as applied to “terrorist” offences.\footnote{Review of the Operation of the Northern Ireland (Emergency Provisions) Act 1978 (Cmd.9222, London, 1984) para. 253.}

By section 38B(4), it is a defence for a person charged with an offence to prove a reasonable excuse for not making the disclosure. The defence of reasonable excuse will often relate to fears of reprisal or reaction going beyond the defence of duress.\footnote{See R v. Sheriff and others [2008] EWCA Crim 2653, para. 53.} Do journalists have a “reasonable excuse” to disregard this legal duty? A reporter may discover information about terrorism by interviewing a terrorist leader or by witnessing a paramilitary display. Arranging, attending, or reporting such events may implicate the journalist in various offences (especially attending a place of training under the Terrorism Act 2006, section 8), but section 38B can involve two further impacts. First, the offence contributes to a “chilling” effect on the reporting of terrorism. Correspondents can expect close attention from the police and hostility and special restrictions from their own superiors. Thus, coverage of Irish terrorism abounded with difficulties and was to some extent suppressed as “guilty secrets.”\footnote{L. Curtis, IRELAND: THE PROPAGANDA WAR (Pluto Press, London, 1984) p 275.} The second effect is the direct threat of prosecution where insufficient weight is given in section 38B to investigative journalism.\footnote{See C.P. Walker, THE PREVENTION OF TERRORISM IN BRITISH LAW (2nd ed., Manchester University Press, Manchester, 1992) pp.141–3.} Such a threat occurred in 1979 and related to a BBC interview with an INLA representative and then the filming (but not transmission) of an IRA road-block in Carrickmore. Both events incurred the wrath of the Attorney-General, who issued a warning to the BBC on the 20 June 1980 that the incidents were of a nature “as constituting in
principle offences…” 139 Despite the threat, no prosecution has ensued.

There is no express exception for the media under section 38B, but the coercion or sanctioning of journalists is subject to article 10 of the European Convention on Human Rights which applies two restraints. The more general is that the highest priority is given to the encouragement of journalism involving political speech. 140 The second aspect of protection is against legal incursions which demand the revelation of sensitive journalistic sources or confidences. 141

In summary, despite the untrammeled breadth of its terms, some restraint has been applied in the usage of section 38B. It serves as a threat rather than the basis for making martyrs out of journalists who, on the evidence of the contempt cases arising from schedule 5 may not be easily convinced to divulge source material. However, the looming threat of prosecution certainly shifts the balance of power in the generally cooperative relations between media and police described earlier.

Section 38B was devised in the days of the IRA, when, geographically and tactically, a more confined conflict was played out between contestants who deeply understood each other. Now, the perception is of “new” terrorism 142 which applies such global savagery that the old restraints of section 38B may also appear outmoded and weak. Another factor to take into account is prolific storage and dissemination of data through the internet. As a result, there is increasing pressure on communication service providers both to impose restraints on their customers and also to keep the security authorities well informed about nefarious customer activities. Furthermore, these duties are very broadly pitched to apply not just to intelligence about offences or potential offences but more generally to extremism and radicalization.

These extraordinary demands, which have not been made of other media, were made explicit in the United Kingdom in connection with the murder of Lee Rigby, a British Army soldier, on 22 May 2013. Those convicted, Michael Adebolajo and Michael Adebowale, drove their car at him and then attempted to behead him. 143 It emerged that Adebolajo was detained under the Terrorism Act 2000, Schedule 7, after deportation on security grounds from Kenya in 2010 but that no further action was taken other than (allegedly) to recruit him as an informant. Aside from these convictions, much of the focus of subsequent inquiries has concentrated on whether the murder could have been prevented,

and two candidate organizations have been under the spotlight – the security agencies and the communications service providers. Much more blame has been attached to the latter than the former. For instance, an Extremism Task Force, formed by the Prime Minister after the killing of Lee Rigby, reported in late 2013. One of its findings was that “Extremist propaganda is too widely available, particularly online, and has a direct impact on radicalising individuals. The poisonous messages of extremists must not be allowed to drown out the voices of the moderate majority.” Action points which it claimed were “agreed” involved:

· work with internet companies to restrict access to terrorist material online which is hosted overseas but illegal under U.K. law
· improve the process for public reporting of extremist content online
· work with the internet industry to help them in their continuing efforts to identify extremist content to include in family-friendly filters
· look at using existing powers to exclude from the U.K. those who post extremist material online who are based overseas

Next, the Intelligence and Security Committee’s Report on the intelligence relating to the murder of Fusilier Lee Rigby found that the security services investigated these individuals on several occasions, but nothing immediately threatening to life had turned up. The agencies knew of their extremism and wanted to use them as informants, especially as they could be pressured as a result of involvement in drug dealing. In short, the agencies acted properly within the resources available – a finding similar to the inquiries into the 7 July 2005 London bombings, even though it was clear that the Woolwich pair were of much higher profile than the 7/7 group. However, the Intelligence and Security Committee do criticize the security agencies in some respects: stronger alarm bells should ring when an individual recurrently becomes of interest; and the Security Intelligence Service must be more proactive and take a greater interest in the activities of cooperating foreign agencies, including allegations of misconduct. Yet the most trenchant criticism is made of the failure of internet companies (especially the unnamed Facebook) for their failure to be more forthcoming with information.

145 Ibid p. 3.
146 Ibid., p.3.
149 An inquiry has been announced: Hansard House of Commons vol.588 col.747 25 November 2014.
Much of the subsequent media and political attention concentrated on the behaviour of Facebook. Several of Michael Adebowale’s multiple social media internet accounts were closed proactively by Facebook and without official request because “they hit triggers...related to their criteria for closing things down on the basis of terrorist content”. Facebook also learned, on completion of a retrospective review of all his 11 accounts, that Adebowale had discussed “in the most explicit and emotive manner” over Facebook’s instant messaging service his desire to murder a soldier. The ISC was nevertheless critical of monitoring procedures by CSPs, though serial investigations by the Security Service were excused as sufficiently thorough, especially because, as pointed out by GCHQ, true intent can be very difficult to discern from online communications. Thus, even if the offending messages had been passed on by Facebook to the security agencies, any reaction by them was far from assured and had been eschewed on several previous occasions. Though Facebook was not wholly forthcoming, their default raises two further jurisdictional issues. One is that their activities (based in the U.S.) are overseen by the U.S. security agencies; thus the Intelligence and Security Committee rather coyly referred to a “partner” foreign agency but without asking whether it knew what was said on Facebook about killing a soldier and whether it consciously failed to pass on that information to the British agencies. A second jurisdictional point is that even in the case of clear default, any proactive legal duty would have limited impact on a company based in the U.S. and any attempt to subpoena information would be laborious (as shown by the Boston Project case). All the same, Sir Nigel Sheinwald has been appointed as Special Envoy on intelligence and law enforcement data sharing in order to secure better transatlantic data sharing.

Putting aside other relevant issues around data privacy, accountability for surveillance, the duty of care to users, and the economic efficiency, were social media companies to be legally obliged to proactively monitor and share all postings of a violent extremist nature with the security authorities, both would be deluged with information and rendered unable to function on an economic basis. Yet, the allure of blaming a foreign internet company rather than home security agencies for failing to avert atrocities seems hard to resist even though it is clear that the Woolwich murder revealed a failure of assessment (perhaps

\[152\] Ibid., para. 390. 
\[153\] Ibid., para. 384. 
\[154\] Ibid., para. 389. 
\[155\] Ibid., para. 393. 
\[156\] Ibid., para. 390. 
understandable and excusable) rather than a crucial lack of information.\textsuperscript{158}

The new head of the Security Service, Andrew Parker, kept up the pressure in his first public speech in early January 2015 by emphasizing the need for powers to access and intercept communications.\textsuperscript{159} His call was soon followed by the Government’s reply to the Intelligence and Security Committee\textsuperscript{160} which was adamant that:

“… Communications Services Providers (CSPs) have a responsibility to ensure their networks are not used to plot terrorist attacks…. we are also pushing CSPs to take stronger, faster and further action to combat the use of their services by terrorists, criminals and their supporters. They are committed to measures that make it easier for their users and the authorities to report terrorist and extremist propaganda. We will build on this to encourage companies to work together to produce industry standards for the identification, removal and referral of terrorist activity.”

By contrast, the government expressed itself “confident that MI5 prioritises available resources and deploys them proportionately to the level of risk represented and as necessary to satisfactorily mitigate the risk, based on the information known at the time.” Yet it seems, by contrast, that CSPs are expected to perform to a higher duty of care with no margin for error or discretion:

“Communications Services Providers (CSPs) have a responsibility to ensure their networks are not used to plot terrorist attacks.”\textsuperscript{161} A more realistic understanding is that even with extensive criminal offences, intrusion into free speech activities, the appointment of extra staff, and extra funding, not all terrorism will be averted. It is unrealistic to expect internet companies to act as better all-seeing and all-doing state spies than the security agencies themselves.

CONCLUSIONS

The modes of treating journalists either as akin to terrorists or in some cases as akin to police officers are not new. The history of demands, threats, and prosecutions extends over several decades. But the adverse stances seem to be growing more prevalent and more insistent. Factors which might explain this trend have broadly been identified as reflecting two vectors. One relates to the perceived nature of terrorism. The “new” terrorism is seen as more threatening and therefore demands greater societal mobilization

\textsuperscript{158} Compare H. Rifkind, Nerds, spies and terrorists, THE SPECTATOR, 29 November 2014; J. Forsyth, The technology giants are breathtakingly irresponsible about terrorism, THE SPECTATOR, 29 November 2014.

\textsuperscript{159} A. Parker, Terrorism, technology and accountability (RUSI, London, 8 January 2015).

\textsuperscript{160} (Cm.9012, London, 2015) pp. 5-6.

\textsuperscript{161} Ibid., p. 5.
and lower tolerance to risk. As a result, counter terrorism is allowed to transcend other values, including the expressive rights of journalists and the privacy rights of their sources. The other vector relates to the perceived nature of the journalism and the media. The official perception seems to be that the media have grown more powerful and should therefore be viewed as more threatening to the interests of counter-terrorism.

Assuming that these trends of hostility to journalism have been established, what should be the reactions? Some international law authorities have expressed concern. In particular, the UN Special Rapporteur on Freedom of Opinion and Expression, the Organization for Security and Cooperation in Europe Representative on Freedom of the Media, the Organization of American States Special Rapporteur on Freedom of Expression and the African Commission on Human and Peoples’ Rights Special Rapporteur on Freedom of Expression and Access to Information issued a Joint Declaration on Defamation of Religions, and Anti-Terrorism and Anti-Extremism Legislation in 2008 which proposed that:

“The definition of terrorism, at least as it applies in the context of restrictions on freedom of expression, should be restricted to violent crimes that are designed to advance an ideological, religious, political or organised criminal cause and to influence public authorities by inflicting terror on the public. The criminalisation of speech relating to terrorism should be restricted to instances of intentional incitement to terrorism, understood as a direct call to engage in terrorism which is directly responsible for increasing the likelihood of a terrorist act occurring, or to actual participation in terrorist acts (for example by directing them). Vague notions such as providing communications support to terrorism or extremism, the ‘glorification’ or ‘promotion’ of terrorism or extremism, and the mere repetition of statements by terrorists, which does not itself constitute incitement, should not be criminalised. The role of the media as a key vehicle for realising freedom of expression and for informing the public should be respected in anti-terrorism and anti-extremism laws. The public has a right to know about the perpetration of acts of terrorism, or attempts thereat, and the media should not be penalised for providing such information. Normal rules on the protection of confidentiality of journalists’ sources of information – including that this should be overridden only by court order on the basis that access to the source is necessary to protect an overriding public interest or private right that cannot be protected by other means – should apply in the context of anti-terrorist actions as at other times.”

A more recent statement of devotion is the European Union’s *Human Rights Guidelines on Freedom of Expression*.\(^{163}\) By paragraph 31, “States should protect by law the right of journalists not to disclose their sources (Unless justified by an overriding requirement in the public interest in conformity with international human rights law) in order to ensure that journalists can report on matters in the public interest without their sources fearing retribution.” Similar sentiments are made in paragraph regarding information and communication technologies. Annex 1 recognises that national security, and so “States must take care to ensure that anti-terrorism laws, treason laws or similar provisions relating to national security (state secrets laws, sedition laws, etc.) are crafted and applied in a manner that is in conformity with their obligations under international human rights law.”

By contrast to this soft law, harder edged international law, such as the already mentioned UN Security Resolution 2178, has tended in the opposite direction, and ideas around offering more protection to journalists, including in conflict zones,\(^ {164}\) have not been delivered.\(^ {165}\)

Turning to domestic safeguards, broad constitutional statements of values, such as freedom of expression, have the virtues of coverage and importance, but they also reflect limits. Even the U.S. First Amendment did not forbid the rendition of the Boston Tapes and has also allowed the material support offences.\(^ {166}\) Likewise, article 10 of the European Convention on Human Rights has proven relatively weak when challenged by operational requirements of counter-terrorism. Within the Human Rights Act 1998, there is the further boost to freedom of expression given by

\(^{163}\) Foreign Affairs Council meeting, Brussels, 12 May 2014.

\(^{164}\) *See* Draft International Conventions for the Protection of Journalists Engaged in Dangerous Missions in Areas of Armed Conflict (UN Doc. A/10147, 1 August 1975).


section 12 which was enacted to “tip the balance” in favour of expression. However, in *Douglas v. Hello! Ltd.*, section 12(4) was not interpreted as according to Article 10 a presumptive priority over other rights. Despite its uncertain impacts, section 12(4) has been used as a precedent in the Counter Terrorism and Security Act 2015, section 31 for giving a special boost to freedom of speech in the application of the “Prevent” duty to universities.

In the light of these experiences, it would seem that, if freedom of expression is to be better safeguarded against counter terrorism, then more specific savings must be inserted into specific policing and court powers. The precedent is the saving for excluded and special procedure journalistic material under sections 11, 13, and 14 of PACE. The same idea is now being advanced in relation in the interception of communications data under the Regulation of Interception of Communications Act 2000. Special savings of this kind may in practical terms require a higher threshold for intervention against journalistic materials and/or may require a stricter level of authorization or supervision of the intervention – such as a judicial warrant. The same devices could be applied for instance in the Terrorism Act 2000, Schedules 5 and 7. Yet, these arguments have been repeatedly raised before the government and Parliament and have been repeatedly rejected.

For the foreseeable future, the value of counter terrorism will consciously continue to be played as a trump card against journalistic data and the interests of free expression and free information in many societies. The three trends now impinging on journalistic activities with reference to counter terrorism seem set to strengthen for now.

---

169 Ibid. at para. 136.