**Chapter 33: Official secrets**

**Chapter summary**

*Official secrets legislation protects national security. It has not been used in recent years to prosecute journalists, but has been used to jail civil servants and others who have given journalists sensitive information. Journalists could be jailed under this legislation. Also, UK governments have used it to gain injunctions to stop leaked material being published. Police could search the home and newsroom of a journalist who is thought to have breached this law, seize their research records and make sustained efforts to discover the confidential source’s identity. There is no ‘public interest’ defence for anyone facing prosecution.*

*Section numbers are used in this extended chapter where such content has that number when summarised in the shorter version of this chapter in the McNae’s book.*

**33.1 Introduction**

The Official Secrets Acts of 1911 and 1989 protect national security and can be used to enforce the duty of confidentiality owed to the UK State by Crown servants or employees of companies doing military and other sensitive work. Crown servants include civil servants, members of the armed services, the police, and civilians working for them. The Act imposes a similar duty on members of the security and intelligence services. Many Crown servants are asked at start of their employment to sign a form acknowledging their obligations under official secrets law – see Useful Websites, below, for an example of such a form. But even if not asked to sign, the obligations apply to these people. Some content of the Acts apply to all citizens.

Part of the legislation was designed to punish spies working for foreign powers, who betray or incite the betrayal of defence, intelligence, and diplomatic secrets, or make vital facilities vulnerable to sabotage.

**Case study:** Royal Navy Petty Officer Edward Devenney, 30, was jailed for eight years in 2012 after he admitted breaching the Official Secrets Act 1911. Aggrieved by failure to gain promotion, he secretly took photographs on a Trident nuclear submarine of code material which enabled NATO communications to remain secret. He rang the Russian embassy, intending to pass this information to Russian agents. He was arrested after meeting two men he thought would be the agents. They were from MI5, the UK’s Security Service (*Metropolitan Police press release*, 12 December 2012).

Official secrets legislation can also punish the leaking of sensitive information to a journalist or a member of the public. Publishing such material makes it available to hostile powers, terrorists and other criminals, and can embarrass the UK’s allies, for example by disclosing diplomatic correspondence.

Using the law to punish leaks is controversial. Attorney Generals – whose legal duties are outlined in 1.6 in *McNae’s* - have approved prosecutions of Crown servants and others who, on grounds of conscience, leaked information to the media to throw light on controversial government policies. In such cases the media and others have questioned whether the prosecution was intended to protect vital state secrets or stifle debate about matters which embarrassed the government. A journalist seen as being an accomplice to a leak of information covered by the Act could be prosecuted for that role, and would commit a separate offence by disclosing it when knowing that the Act protects it. This leaves journalists and editors open to prosecution for publishing or circulating the information.

A Crown servant, or someone else with an obligation of confidentiality under the Act, who accidentally leaves sensitive information where members of the public may find it can also be punished.

**33.2 The law’s consequences for journalists**

Journalists were jailed in 1916 and 1932 for offences under the 1911 Act. But no journalist has been successfully prosecuted under official secrets law, let alone jailed, for many years.

**Case study**: In 2013 Edward Snowden leaked to journalists material he copied when he was a contractor with the USA’s National Security Agency. After travelling to Hong Kong, Snowden publicly revealed he was the leaker, saying he wanted to expose the extent of the USA’s and UK’s secret surveillance of the world’s communications systems. *The Guardian*, drawing on this material, revealed some detail of the UK’s secret co-operation with the USA in this surveillance, including of emails. A former head of the UK’s surveillance base GCHQ was quoted in *The Times* as saying that it had to be assumed that Snowden’s travels meant UK intelligence files had been hacked from his computer by China and Russia, and that this was ‘the most catastrophic loss to British intelligence ever’. But *The Guardian* was not charged with breaching official secrets law for publishing some of Snowden’s material, although a threat of legal action meant that the newspaper complied with a demand by Government officials that it destroy computer hard drives containing files he leaked (*The* *Guardian*, 10 June, 19 and 20 August 2013; *The Times,* 11 October 2013). The online chapter 40 on [www.mcnaes.com](http://www.mcnaes.com), ‘Terrorism and the effect of counter-terrorism law’ refers to controversial use of counter-terrorism law to detain David Miranda at Heathrow airport. He is the spouse of journalist Glenn Greenwald who worked with *The Guardian* to produce news articles based on information from Snowden. See also material below about how *The Guardian’s* publication of Snowden’s revelations affected the DA Notice system.

Prosecutions under the 1911 and 1989 Acts can be brought only by or with the consent of the Attorney General, except in cases relating to crime or special investigation powers, when the Director of Public Prosecutions’ consent is needed.

The reasons for the reluctance to prosecute journalists are discussed below. Journalists need to be aware of the Acts, to be ready to protect their sources because this—as ch. 34 emphasises—is a moral obligation. A journalist may not be jailed for publishing a story, but the source may well be jailed for disclosing that information to the journalist. Police might raid a journalist’s home, newsroom or office in the search for a source’s identity, and a journalist may be arrested and threatened with prosecution. An injunction might stop the journalist publishing information. See below. The Acts are considered to have a chilling effect on journalists investigating issues which might be in the public interest. *McNae’s* ch. 34 and the online ch. 40 explain police powers to seize material or require it to be surrendered.

**Examples of journalists investigated**

In 1977 journalists Crispin Aubrey and Duncan Campbell were arrested in London by Special Branch police investigating alleged breaches of the Official Secrets Act 1911. Campbell had published articles revealing the mingled nature of the UK’s civil and military communications systems, and how the state’s intelligence-gathering at home and abroad involved the interception of radio signals and tapping phones. Both journalists were charged with breach of the Act – the statute is explained below - and consequently were defendants in what became known as ‘the ABC trial’. Although both were convicted, the judge made clear he felt their offending was minor, because each was given a conditional discharge. The Additional Material for chapter 15 on [www.mcnaes.com](http://www.mcnaes.com) provides further detail of this trial, and outlines how this prosecution became discredited.

In 1998 Ministry of Defence police raided the home of Tony Geraghty, the former *Sunday Times* defence correspondent, after publication of his book *The Irish War*, which disclosed extensive use of computerised surveillance by intelligence agencies in Northern Ireland*.* He was arrested and charged with an offence under the Official Secrets Act 1989. It was not until a year later that the charge against him was dropped.

In 2000 Julie-Ann Davies, a broadcast researcher, was arrested and questioned on suspicion of a possible breach of the Act on the basis that she had communicated with David Shayler, a former MI5 officer who had given *The Mail on Sunday* security-related information. She was not prosecuted.

In 2003 armed police raided the home of Liam Clarke, the Northern Ireland editor of *The Sunday Times*, and arrested him and his wife Kathryn Johnston, following publication of an updated version of their book *From Guns to Government*, which contained transcripts of tape-recordings, made in a joint police/MI5 surveillance operation, detailing bugged telephone conversations acutely embarrassing to the UK Government. The couple were detained at their home for five hours. Officers also raided the Belfast office of *The* *Sunday Times*, battering the door down. Later the police admitted the raids were unlawful because, although they obtained a search warrant under the Police and Criminal Evidence Act 1984 (PACE), it was authorised by a magistrate, not by a Crown court judge as the law at that time required. PACE is explained in 34.6 in *McNae’s*. In the High Court in Belfast Mr Justice Kerr quashed the warrant and ordered the police to pay the paper’s costs of its application for judicial review. In 2006 the two journalists were reported to have received a ‘five-figure’ sum from the police in settlement of a claim for false imprisonment arising from the raid on their home (*Press Gazette*, 20 September 2006).

In 2005 Attorney General Lord Goldsmith issued a warning to newspapers after *The Daily Mirror* published a story headlined ‘PM halted Bush plan to bomb Arab TV channel off the air’. The story began: ‘George Bush’s plot to bomb an Arab TV station in friendly Qatar was crushed by Tony Blair, who feared it would spark horrific revenge.’ The paper said the story was based on a leaked memo which detailed minutes of a conversation in which Mr Blair and Mr Bush discussed the Arabic TV broadcaster Al-Jazeera. The broadcaster had angered the US and British Governments by showing footage of dead soldiers and others killed in the Iraq war. The Attorney General warned that the media would be contravening official secrets law if it published the memo’s contents. Commentators suggested that Lord Goldsmith ‘read the riot act’ to the media because of political embarrassment caused by this sensitive leak of face-to-face exchanges between the prime minister and the US president. The *Mirror*’s editor was threatened with prosecution under the Official Secrets Act 1989 and with an injunction unless he confirmed that the paper would not publish further details. ‘We have essentially agreed to comply,’ the editor said (*The Daily Mirror,* 22 and23 November 2005*; Guardian*, 23 and 24 November 2005; *Media Lawyer*, 28 November 2005).

In 2011 the Metropolitan police dropped an attempt to order *The Guardian* to reveal confidential sources for stories relating to *The News of the World* phone-hacking scandal (which is outlined in 35.1 in *McNae’s*). The police application to a judge for a ‘production order’ was formally being made under PACE, but with an assertion that *Guardian* reporter Amelia Hill could have committed an offence under the Official Secrets Act 1989 by inciting an officer from Operation Weeting – the police investigation into phone-hacking – to reveal information. Media lawyers expressed astonishment at the police resorting to the Official Secrets Act, in particular because it had been *The Guardian* which had exposed the police’s earlier failure to fully investigate the hacking scandal, a revelation clearly in the public interest. In the face of growing controversy about this attempt to require the reporter to identify sources of information, and that official secrets law was being cited, the police withdrew the application for a production order. The Director of Public Prosecutions Keir Starmer QC said that the Crown Prosecution Service had not been contacted by the police before the application was made. Hill was interviewed under caution by police but not charged with any offence (*The* *Guardian*, 16, 19 and 20 September 2011, and 29 May 2012).

**The fate of sources**

Sources are generally dealt with more severely than journalists. A Crown servant who is found to have leaked sensitive information to the media will almost certainly be sacked, even if there is no prosecution. Anyone convicted of leaking material ruled to be covered by official secrets legislation could be jailed.

Former MI5 officer David Shayler was jailed for six months in 2002. Stories he gave *The* *Mail on Sunday* in 1997 included the disclosure that the Government kept secret files on some Labour politicians. The newspaper published the story, but was not prosecuted. Shayler also said that MI5 had prior knowledge of a terrorist attack on the Israeli embassy, but failed to react. He also alleged that MI6 officers had plotted to assassinate the Libyan leader, Colonel Gaddafi. At one stage Shayler was arrested in France and held without charge for four months while the UK Government attempted – unsuccessfully - to extradite him. He returned to the UK voluntarily in 2000, and was then arrested and charged with three offences under the 1989 Act. He unsuccessfully appealed to the Court of Appeal and the House of Lords, see below.

In the Al-Jazeeracase, referred to above, former civil servant David Keogh and Leo O’Connor, who had worked as an MP’s researcher, were jailed in 2007 for six months and three months respectively for leaking the memo received by the *Mirror*.

In 2007 Thomas Lund-Lack, who worked for the Metropolitan Police’s counter-terrorism command, was jailed for eight months for ‘wilful misconduct in a judicial or public office’, a charge which arose after he leaked documents to *Th*e *Sunday Times* about the threat Al-Qaeda posed to the UK. A charge under the Official Secrets Act 1989, which he denied, was dropped.

In 2008 charges under section 3 of the 1989 Act against Foreign Office civil servant Derek Pasquill were dropped shortly before he was due to be tried at the Old Bailey on charges of having leaked documents to both *The Observer* newspaper and *New Statesman* magazine. Some of the documents concerned the controversial ‘rendition’ of terrorist suspects, and some the Government’s policy of engaging in dialogue with hard-line Islamic radicals. The Government’s counsel told the judge that there was no longer a realistic prospect of conviction (*Media Lawyer*, 9 January 2008). It was later reported that internal Foreign Office papers revealed that senior officials had privately admitted that instead of harming the UK’s interests, the leaks of some of the documents had helped provoke a constructive debate about the dialogue policy.

In 2003 Katharine Gun, a translator at the Government’s GCHQ communications centre, was charged under section 1 of the 1989 Act after leaking the content of an email to someone who passed it on to *The Observer* newspaper. The email was a request from US officials for the phones of some nations’ diplomats at the United Nations to be tapped. Ms Gun was sacked. The case against her ended the next year, when the prosecution decided to offer no evidence. The Attorney General told Parliament that prosecution counsel had decided there was no longer a realistic prospect of conviction. In 2019 a film, *Official Secrets*, has its cinema premiere. This was a drama adaptation about what happened, in which Keira Knightley acted the part of Gun.

In 1998 Stephen Hayden, a Royal Navy chief petty officer, admitted breaching the Act by selling *The Sun* newspaper information that Iraqi leader Saddam Hussein considered a biological warfare attack on the UK involving anthrax. Hayden pleaded guilty and was jailed for a year.

In 1985 a jury acquitted Clive Ponting, a senior civil servant who was charged under official secrets legislation after giving an MP information about the controversial sinking of the Argentine battleship the *Belgrano* in the 1982 Falklands war.

In none of these cases in which sources were prosecuted was any media organisation or journalist prosecuted. With the exception of Tony Geraghty, no journalist has been prosecuted under the UK official secrets law for nearly 40 years. And, as explained, the case against him was dropped.

**The chilling effect is widespread**

Journalists should probe the conduct and performance of state agencies, not just accept the government’s accounts of its policies and actions. There is little doubt that journalism’s watchdog role suffers from ‘the chilling effect’ of official secrecy law, to the detriment of democratic debate. It is not only journalists who believe this. In 2003 Rear Admiral Nick Wilkinson, then secretary of the Defence, Press and Broadcasting Advisory Committee – now known as the DSMA committee, see below- said that the 1989 Act had a ‘pernicious influence’ on dialogue between officials and the public, including the media, and was in need of a ‘post-Cold War review’. He said the review was necessary not so much because of the content of the Act or its use in litigation, but because of its influence on government communications in the widest sense, as it induced in officials an attitude of ‘How little can I get away with saying?’ rather than ‘What must I really not say at present?’ Rear Admiral Wilkinson said: ‘This attitude is only partly a reflection of the civil service’s tradition of serving the government of the day: it is largely a reflection of the instinct of self preservation inherent in all bureaucracies’

Case study: Officials continue to suggest that journalists or media organisations could be prosecuted under the Official Secrets Act 1989. In 2019 the *Mail on Sunday* published leaks from confidential memos to the Prime Minister’s office in which the UK’s ambassador in Washington, Sir Kim Darroch, had described US President Donald Trump as 'inept', 'insecure' and 'incompetent'. The leaks led to Sir Kim resigning because his chances of maintaining harmonious relations with Trump were destroyed, as Trump made clear. Neil Basu, an Assistant Commissioner with the Metropolitan police, which began investigating who leaked the memos, stirred a controversy by saying that publishing their content ‘knowing the damage they have caused or are likely to cause’ may be a ‘criminal matter’. But he later said he had ‘no intention of seeking to prevent editors from publishing stories in the public interest in a liberal democracy’ (*Mail Online,* 6, 10 and 15 July 2019*; Press Gazette,* 15 July 2019). When this Additional Material was finalised in 2020, there had been no prosecution arising from those leaks.

**Case study:** Official secrets law continues to be cited when officialdom wants to deter ‘whistleblowers’ from speaking to the media. In 2015 *The* *Grimsby Telegraph* reported from an unnamed police source that, after a ‘restructure’ in staffing, on some 3am – 7am shifts there were only four officers working in the whole of North East Lincolnshire. Humberside Police and Crime Commissioner Matthew Grove denied the claim, telling the paper: ‘If any police officers are telling you the number of officers on duty, they are breaking the Official Secrets Act and becoming criminals.’ *The Times* described as ‘ridiculous’ this idea that ‘junior officers who raised the alarm about inadequate night staffing’ had acted criminally by doing that. Mr Grove, faced with such criticism, later said: ‘I signed the Official Secrets Act on taking office as Commissioner, and felt that to provide sensitive information such as that disclosed would breach the principles of the Act.’ He added: ‘I would never try to ‘gag’ police officers from giving their views as has been implied, but ask them to consider the wider impact on the public and their colleagues before they do’ *(The Grimsby Telegraph,* 15 May and 5 June 2015, *The Times* and *Press Gazette*, 4 June 2015).

**33.2.1 Reluctance to prosecute journalists**

As this chapter makes clear, a source is more likely to be prosecuted under official secrets law than is the journalist who receives and discloses information from the source. The reluctance to prosecute journalists is partly an effect of the legislation. Section 5 of the 1989 Act contains defences which journalists can use but sources cannot. For example, the journalist has a defence that disclosure of the information was not ‘damaging’ to state interests – for example, to the work of the intelligence services.

But a journalist might be found guilty of inciting or of aiding and abetting the source to commit an offence under the terms of section 1. This was the section under which David Shayler was prosecuted. Alarmed by the legal position, seven national newspapers made representations to the Court of Appeal when it was hearing Shayler’s appeal, and the Lord Chief Justice, Lord Woolf, after pointing out that section 5 of the Act provided protection to the media that was not available to Shayler, said that only in exceptional circumstances would the Attorney General need to authorise a prosecution of the media for incitement to commit an offence under section 1.

John Wadham, who was Shayler’s lawyer when director of the civil rights organisation Liberty, said of the lack of prosecutions of journalists: ‘It is partly because governments don’t like to be seen to be trying to put journalists in prison and partly because juries are less sympathetic to civil servants – who are employed to keep their mouths shut, who are aware of the rules but break them, and who breach the trust with employers and colleagues – compared with journalists, who are paid to find things out and publish them.’

**33.3 The 1911 Act**

Section 1 of the Official Secrets Act 1911 is concerned with spying, but journalists should know about it. The section makes it an arrestable offence, carring a penalty of up to 14 years’ imprisonment, to do any of the following ‘for any purpose prejudicial to the safety or interests of the state’:

(a) approach, inspect, pass over, be in the neighbourhood of, or enter any prohibited place (see below);

(b) make any sketch, plan, model, or note that might be or is intended to be useful to an enemy;

(c) obtain, collect, record, or communicate to any person any information that might be or is intended to be useful to an enemy.

Offences under (c) are regarded as most relevant for journalists. This section was used in the charges against the journalists Crispin Aubrey and Duncan Campbell, see above, but has not been used against any journalist since.

Section 3 of the 1911 Act gives a lengthy definition of a ‘prohibited place’ as including, for example, ‘any work or defence, arsenal, naval or air force establishment or station, factory, dockyard, mine, minefield, camp, ship, or aircraft’ and ‘any telegraph, telephone, wireless or signal station, or office’ when any such property is used by the State. **Statutory instruments** have added British Nuclear Fuels plc and Atomic Energy Authority sites to the list of prohibited places. The Energy Act 2008 added any site where there is equipment or software for enriching uranium, or information about the process. These additions apparently reflect fears that terrorist groups want to build a nuclear bomb, or a ‘dirty’, radioactive one, or that rogue nations may seek to spy on these facilities or that they are targets for sabotage.

As can be seen, the definition of a prohibited place is wide. The media must remember that taking photos or gathering information outside or near a prohibited place, even in routine news coverage of events such as peace protests, could be held to be a breach of the Act, for example, if material gathered and published jeopardises security at a defence base. Also, the Serious Organised Crime and Police Act 2005 makes it a criminal offence to trespass in any of the nuclear and military sites designated as ‘protected sites’ in associated statutory instruments – see 36.3 in the Additional Material for ch. 36, on this website.

The 1989 Official Secrets Act, see below, replaced section 2 of the 1911 Act, which was known as the ‘catch-all section’ because of the wide range of information covered. Under section 2, no Crown servant or government contractor could lawfully make an unauthorised disclosure of any information which he/she had learned in the course of his/her job. The section potentially made it a crime to disclose, for example, the number of cups of tea drunk each week in a government department or the details of a new carpet in a Minister’s room. Under the section it was an offence for a person to merely *receive* such information, if it had been disclosed without authority. This was the part of the 1911 Act with which journalists were most frequently threatened. But in cases in the 1970s and 1980s the Attorney General failed to persuade juries to convict defendants prosecuted under section 2. The 1989 Act abolished the section.

**Duty to name sources**

Section 6 of the 1911 Act enables a chief officer of police to require a person to divulge information, which could include the identity of a source, when the officer believes an offence under section 1 has been committed. Refusal to comply is an offence.

**33.4 The 1989 Act: the journalist’s position**

The Official Secrets Act 1989 makes it an offence to disclose information as defined in six categories:

1) security and intelligence (section 1 of the Act);

(2) defence (section 2);

(3) international relations (section 3);

(4) crime (section 4);

(5) information on government phone-tapping, mail interception, or other communications (section 4 also);

(6) information entrusted in confidence to other states or international organisations (section 6).

For convenience, these can be referred to as Classes 1 to 6.

Section 5 of the Act says that a person – for example, a journalist – commits an offence if he/she discloses without lawful authority information protected by the Act, knowing or having reasonable cause to believe that it is thus protected against disclosure, if he/she received it from a Crown servant or government contractor (a) without lawful authority, or (b) in confidence, or received it from someone else who received it in confidence from such a person.

‘In confidence’ means either that the discloser - in this example, a journalist - has been told the information is being given to him/her in confidence, or the circumstances are such he or she could reasonably suppose the information would be held in confidence.

In four of the classes of information given above, the prosecution in a case against a journalist would have to prove that the disclosure is damaging to state interests and that the journalist knew, or had reasonable cause to believe, that the disclosure of this information would be damaging, as defined in the Act. The test of what is damaging differs according to the class of information.

This law is explained further in the table ‘Will your story contravene the Official Secrets Act 1989?’, also on the *McNae’s* website.

For two of the classes of information the prosecution does not have to prove that disclosure was damaging, because the Act assumes that it is. Suppose, for example, a journalist publishes a story based on information from a policeman that a senior opposition MP’s telephone is being tapped under warrant but for dubious reasons. A policeman is a Crown servant, and the information relates to government phone-tapping, covered in section 4 of the Act (Class 5 in the table). The prosecution does not have to prove damage as damage is assumed in respect of the actions of both policeman and journalist. Neither, under the terms of the Act, can successfully plead for acquittal on grounds that the phone-tapping was improperly authorised and that they believed disclosure of such impropriety was in the public interest.

Under the Act, for a journalist’s source the situation is much worse in that a source can be guilty of an offence, without any proof of damage, in many more situations than the journalist (see the table). For example, no proof of damage is required if, without authority, a member of the security or intelligence services discloses information relating to security or intelligence that came into his/her possession because of his/her work as a member of any of those services.

In most cases (but see table) the journalist does not commit an offence if the person from whom he/she received the information, although a government contractor or a person to whom it was entrusted in confidence, was not a UK citizen or the disclosure did not take place in the United Kingdom, the Channel Islands, the Isle of Man, or a British colony.

* It is also an offence under section 5 of the 1989 Act to disclose any information which the discloser knows or has reasonable cause to believe came into his/her possession as a result of a breach of section 1 of the 1911 Act, see above.

Section 6of the 1989 Act covers the disclosure of information communicated in confidence to other states or international organisations, and there are no requirements that the information must have been disclosed originally by Crown servants or government contractors. Journalists or any other members of the public commit the offence by disclosing such information when it relates to security or intelligence, defence, or international relations. The information must have come into their possession as a result of being disclosed, whether to them or others, without the authority of the state or organisation or, in the case of an organisation, of a member of it. But the prosecution also has to prove that the defendant knew, or had reasonable cause to believe, that the information was of the type covered by the section, and that it had come into his/her possession in the way mentioned, and that its disclosure would be damaging.

* Section 8makes it an offence for a person to fail to comply with an ‘official’ order to return a document, where disclosure of the document would be an offence under the Act.

**33.4.1 Damage test but no public interest defence**

* The law permits no ‘public interest’ defence in official secrets cases. Also, the information can still be legally classed as secret even if it has already been published. The key test on whether an offence has been committed by a journalist may well be the ‘damage test’.

As indicated above, the degree of damage (by disclosure) necessary for conviction under the 1989 Act varies according to the class of information and the category of person accused (see table ‘Will your story contravene the Official Secrets Act 1989?’). Though the Act can catch journalists and members of the public, it is directed particularly at members of the security services, Crown servants, and government contractors.

Consider these examples:

(1) A journalist writes a story based on information received from a member of the security services (Class 1 information) that members of the services have been involved in illegal activities. The Act assumes that any disclosure about security by a member of the security services is damaging, and such a person cannot defend himself/herself on the ground that the disclosure was not damaging. On the other hand, a Crown servant or a government contractor who makes a disclosure on the same subject is guilty only if the disclosure is proved to be damaging. The Act says that in this context a disclosure is damaging if:

(a) it causes damage to the work of, or of any part of, the security and intelligence services; or

(b) it is of information which is such that its unauthorised disclosure would be likely to cause such damage or which falls within a class or description of information the unauthorised disclosure of which would be likely to have that effect.

If a journalist is accused of making a disclosure about security the prosecution has to prove damage and the test is the same as that for a Crown servant, whether the journalist got the information from a Crown servant or a member of the security services.

(2) In defence matters (Class 2 information), the prosecution always has to prove the disclosure was damaging. See the table for what makes a disclosure on a defence matter damaging. This same test of damage would be applied to a Crown servant making a disclosure on defence matters or a journalist writing a story based upon it. Note it is again sufficient to show that the information was ‘such that’ its unauthorised disclosure would be likely to be damaging, but that there is no ‘class’ test as in the example at (1).

If the prosecution has to prove disclosure is damaging, the test is expressed in every case in very wide terms. In all cases in the Act where a definition of damage is given it includes the ‘such that’ formula, see b) above.

**The onus of proof**

Any journalist who risks being prosecuted under the Act will take a keen interest in who has to prove what. As with the test of damage, the onus of proof in the matter of damage also varies according to the class of information and the category of the person accused.

If a member of the security services makes a disclosure about his/her work the court will assume damage, and no proof of damage is necessary. If a Crown servant or government contractor makes a disclosure about security, the prosecution has to prove the disclosure was damaging, but the Crown servant has a defence if he/she can prove that he/she did not know or had no reasonable cause to believe that it would be damaging. In the case of a journalist making a disclosure about security, the prosecution must prove not only that the disclosure was damaging, but also that the journalist knew or had reasonable cause to believe that it would be damaging – the onus of proof is on the prosecution.

(Where, in the accompanying table, knowledge of the damaging nature of the information is part of the offence, and the onus is on the prosecution to prove it, this is included in column 3. Where lack of knowledge is a defence, which the defendant has to establish, this is included in column 5.)

**Jury may acquit, after recognising public interest ‘by the back door**

The lawyer David Hooper, author of the book *Official Secrets; the use and abuse of the Act*, has said that he believes the damage test may let in public interest ‘by the back door’.

Suppose the journalist being prosecuted had exposed a scandal concerning state activities. A jury, when deciding whether the journalist knew the disclosure would be damaging to the state’s interests, may – whatever the law says – choose to take the public interest in the material being published into account when arriving at a verdict.

**Misconduct in public office**

It should be remembered that, even if material leaked to a journalist is not covered by official secrets law, a leaker who is a public official – for example, a police officer, prison officer, civil servant or someone employed by the armed services - could be charged with the common law offence of misconduct in public office (as Thomas Lund-Lack was, see above).

In such a case, a journalist who paid for the material or otherwise incited the leak could be charged with conspiracy to commit this offence or aiding and abetting it. See 35.2.1 in *McNae’s* for explanation of this offence.

**Official secrecy versus freedom of expression**

It has been suggested that official secrets legislation is susceptible to challenge under the Human Rights Act 1998, which came into effect in October 2000, incorporating the European Convention on Human Rights into UK law. See 1.3 in *McNae’s* for explanation of the Convention’s general effect. Any court determining a question in connection with Convention rights – and for journalists these are most likely to be those in Article 10 which protects freedom of expression and to impart information – must construe existing legislation as far as possible to conform with the Convention rights. Article 10 rights may be restricted ‘in the interests of national security’, according to Article 10(2). But it makes clear that the exceptions (that is, the specified restrictions on Article 10 rights) listed in this subsection apply only so far as is ‘necessary in a democratic society’. The European Court of Human Rights (ECtHR) has ruled that reliance on such exceptions must answer a ‘pressing social need’ (in the context of official secrets law, this is likely to be a particular need to uphold an aspect of national security). That court has also ruled that interference with Article 10 freedoms, even if lawful, must be ‘proportionate to the legitimate aim pursued’.

Lawyers for David Shayler, see above, argued strongly that the Convention gave him a defence, in that Article 10 rights protect publication which is ‘in the public interest’. In a preparatory hearing in May 2001 before his trial, it was argued on his behalf that the disclosures he made were in the public interest because they exposed serious illegality by the UK secret services and/or were necessary to avert threat to life and limb and serious damage to property (the ‘necessity’ argument’ – see also below, under Useful Websites, the House of Commons Library Briefing Paper ‘The Official Secrets Acts and Official Secrecy’). But the trial judge said the 1989 Act did not contain any exception to permit disclosure in the public interest. He ruled that all that the prosecution needed to prove was that a member or former member of the security service had (without authority) disclosed information that he/she acquired through his/her work. The judge also ruled that the restriction on disclosing secret information and the related criminal sanction were proportionate to the legitimate aim of protecting national security and necessary in a democratic society, and accordingly did not constitute violations of Article 10. In September 2001 the Court of Appeal dismissed Shayler’s appeal and in 2002 the House of Lords dismissed his further appeal.

Lord Bingham of Cornhill, giving the leading judgment in the House of Lords, recognised that restrictions on freedom of expression had to be carefully scrutinised by the courts to ensure that they were proportionate to the aim they sought to further. But he said that an absolute ban against a member of the security service disclosing information was necessary to protect national security. He added that it was also important to take into account the safeguards built into the Act that allowed a security officer to report unlawfulness and irregularity to superior officers and Ministers with the power and duty to take effective action. An officer could also seek authorisation to disclose information to the general public and could challenge, by judicial review, a refusal to give it.

Shayler’s stance was that there were no effective steps which could be taken through official channels to address his concerns and he had not therefore sought authorisation. Lord Bingham’s view was: ‘If a person who has given a binding undertaking of confidentiality seeks to be relieved, even in part, from that undertaking he must seek authorisation and, if so advised, challenge any refusal of authorisation. If that refusal is upheld in the courts it must, however reluctantly, be accepted’ (*R v David Michael Shayler [2002]* HL 11).

In essence, in key rulings on media investigation of matters relating to national security, UK judges have said that the Government, rather than the media, knows what information if published could damage national security, because the Government officials have fuller knowledge than the media of security and intelligence operations, and about what ‘jigsaw’ pieces of information could aid enemies of the state. For example, this position was set out in 2014 by the High Court in the *Miranda* case, outlined in 40.9 in *McNae’s* online chapter 40: ‘Terrorism and the effect of counter-terrorism law’.

**Penalties**

Penalties for an offence of disclosure under the 1989 Act are a maximum of two years’ imprisonment or a fine or both. If the case is tried summarily (by magistrates) the maximum is six months or a fine or both.

**The use of injunctions**

Official disillusionment with section 2 of the 1911 Act as a means of stopping leaks of information led to UK governments changing tack from the 1980s, in that they began using injunctions to ban publication of leaked material on grounds of breach of confidence. This led to the media being silenced on occasion without a criminal prosecution – that is, without the risk of ministers suffering political embarrassment through a jury’s decision that the publication was lawful. Injunctions are granted by judges sitting alone, and it is a contempt of court to disobey such an order, which can be punished by a jail term of up to two years and/or a fine unlimited by statute. In 1985 the UK Government used the law of breach of confidence when attempting to stop publication of information acquired by Peter Wright during his former job as a senior officer of the Security Service, MI5. He planned to make money by selling his memoirs – a book called *Spycatcher*. See 26.3 in *McNae’s* for more detail of the *Spycatcher* proceedings.

After *The* *Mail on Sunday* published David Shayler’s allegations, see above, the Government obtained an injunction forbidding him and the newspaper from revealing any further information unless formally authorised. But the High Court in 2000 rejected a police application for an order that *The* *Guardian* and the *Observer* shouldhand over all files, documents, and records they had relating to Shayler (*R v Central Criminal Court, ex p Martin Bright* [2001] 2 All ER 244).

**33.5 The media may be excluded from secrets trials**

Section 8 of the Official Secrets Act 1920 allows for the exclusion of the public and the media from secrets trials when publication of evidence would be ‘prejudicial to the national safety’. There is no generally recognised definition of national safety (or national security). The Act says a court must sit in open session when sentencing a convicted defendant.

**The Law Commission’s proposals**

In 2017 the Law Commission published a consultation report which reviewed official secrecy law, and made proposals to change it. One proposal was that the maximum penalty for breaching official secrets law should be increased from the current maximum jail term of two years which, the Commission said, might not reflect sufficiently the severity of some breaches. It pointed out that in Canada the maximum penalty is a jail term of 14 years. The Commission also proposed that the requirements under the 1989 Act for the prosecution to prove disclosure of material was ‘damaging’ should be abolished, and gave arguments for this. For example, the Commission suggested new law so that ‘a person commits an offence if he or she intentionally makes an unauthorised disclosure of information relating to security and intelligence, knowing or having reasonable grounds to believe that that disclosure is capable of damaging security and intelligence.’ The Commission rejected the idea that a defence should be created in statute to protect journalists for publication in the public interest of material which state agencies deemed an official secret. The Commission said: ‘Our provisional conclusion is that the public interest is better served by providing a scheme permitting someone who has concerns about their work to bring it to the attention of the independent Investigatory Powers Commissioner, who would have statutory abilities to conduct an investigation and report.’ This would be expansion of the role of the Commissioner. (For an outline of the Commissioner’s existing roles as regards protection of journalists’ confidential sources, see 34.3.1 in *McNae’s,* and the Additional Material for chs. 34 and 40 on www.mcnaes.com. See Useful Websites, below, for the Commissioner’s Office site.)

The Commission’s report was fiercely criticised by organisations representing journalists and the media, and others. For example, the News Media Association said: ‘The Law Commission’s consultative proposals, if adopted, would have deeply disturbing consequences for the public right to know and the role of the press in public scrutiny of the state.’ It also said: ‘The NMA is particularly concerned about the Law Commission’s proposals to shift the focus of relevant OSA 1989 offences from proof of disclosure likely to cause damage, to enable the prosecution, conviction and imprisonment for longer term of those whose disclosures did not cause harm - and were not likely to do so. …The damage tests in the 1989 Act are vital protections for freedom of expression, allowing disclosures that are unlikely to harm, enabling public attention properly to be alerted to official misconduct or mismanagement or abuse of powers.’

See Useful Websites, below, for the Commission’s report, and for some of the responses to it.

**33.6 Defence and Security Media Advisory Notice system**

In 2015 what was the Defence Press and Broadcasting Advisory Committee was reformed to become the Defence and Security Media Advisory (DSMA) committee. The committee is, as its predecessor was, the head of a joint government/media system through which the news media and other publishers – for example, when planning to publish a news article or a book, or to broadcast a news item - can get specific guidance on how to avoid inadvertent disclosure of information damaging to the UK’s national security and defence.

The committee comprises four senior officials of the Cabinet Office, Ministry of Defence, the Home Office, and the Foreign Office, and 17 nominees from newspapers, magazines, news agencies, broadcasting and book organisations. The chair is the Ministry of Defence’s Director General Security Policy.

The committee has five standing ‘notices’ giving general guidance. These are widely known as D-Notices (defence notices). Until 31 July 2015 they were officially called DA Notices (‘defence advisory’) but are now officially called DSMA-Notices. They describe the types of subject matter which the Government and media members of the committee consider may damage national security if published. These standing DSMA-Notices are distributed to national, regional and local newspapers, radio and television organisations, major internet service providers, and some publishers of periodicals and books on defence and related subjects. They can be read in full on the committee’s website - see Useful Websites, below - and cover the following subjects:

1. military operations, plans and capabilities;
2. nuclear and non-nuclear weapons and equipment [for defence and counter-terrorism];
3. m[ilitary counter-terrorist forces, special forces and intelligence agency operations, activities and communication methods and techniques](https://dsma.uk/notice/military-counter-terrorist-forces-special-forces-and-intelligence-agency-operations-activities-and-communication-methods-and-techniques/);
4. identification of sensitive installations;
5. [personnel who work in sensitive positions](https://dsma.uk/notice/personnel-and-their-families-who-work-in-sensitive-positions/), and their families;

The permanent secretary of the committee (known as the DSMA-Notice secretary) is normally a retired senior officer from the armed forces. The current secretary is Brigadier Geoffrey Dodds. His contact details are on the committee’s website, as are the names of all the committee members. When the secretary learns of media interest in any of the DSMA-Notice areas, he contacts the editor, publisher, or programme maker to offer advice. Editors, defence correspondents, other journalists, and authors can initiate contact to consult him to check whether information being considered for publication comes within a sensitive area.

The committee’s minutes, which can be read on its website, showed that in the year to November 7, 2019 its secretariat dealt with 158 enquiries and requests for DSMA Notice advice.

**Case study:** The minutes of the committee’s meeting of 16 May 2019 show that its secretary, Brigadier Dodds expressed concern that on December 21, 2018, ‘one UK media member’ tweeted live commentary about a special forces night operation to secure the safety of the crew of a ‘stricken maritime vessel in the Thames estuary’ who were under threat from a group of illegal immigrants. The minutes say: ‘Such live *before and after* reporting runs counter to the advice offered under DSMA standing notice 3. The tweeter was reminded of the implications of such reporting at the time. The Secretary subsequently wrote to all Committee members at the request of the Secretary of State for Defence to invite them to remind the wider UK media community, at an appropriate opportunity, of the dangers of live and *before and after* reporting of such operations.’

Part of standing notice 3 asks the media to check with the committee’s secretariat before disclosing methods and techniques of special forces. The aim is to avoid publication of detail which might compromise their future effectiveness. The estuary incident referred to in these minutes was reported by one newspaper under the headline: ‘Special forces retake cargo ship after stowaways threatened staff.’

**33.6.1 Review after the Snowden affair**

*The Guardian’s* publication in 2013 of some of the intelligence information stolen by Edward Snowden, see above, led mainstream organisations in the UK news media and the Government to consider if the committee was ‘fit for purpose’ in the internet age.

The secretary’s report in the committee’s minutes from that time say: ‘This event was very concerning because at the outset *The Guardian* avoided engaging with [what was then] the DA Notice System before publishing the first tranche of [Snowden] information. As a member of the Newspaper Publishers Association (NPA), *The Guardian* was obliged to seek (but not necessarily to accept) DA Notice advice under the terms of the DA Notice code. This failure to seek advice was a key source of concern and considerable efforts had been made to address it. There was also an important international dimension which played into the already complex equation. *The Guardian* was not the only newspaper involved in disclosing Snowden’s information, as the *New York Times* (NYT) was also publishing the same details in parallel. This meant that - even if *The Guardian* had sought and followed DA Notice advice - the highly sensitive information about GCHQ could still have been disclosed and once disclosed would immediately be widely repeated across the internet. This fact complicated subsequent dealings with *The* *Guardian*. Towards the end of July [2013] *The* *Guardian* had begun to seek and accept DA Notice advice not to publish certain highly sensitive details, and since then the dialogue with the [committee’s] Secretariat had been reasonable and improving. The events of the last few months had undoubtedly raised questions in some minds about the [DA Notice] system’s future usefulness.’

[Alan Rusbridger, the editor of *The Guardian*, has said that the DA Notice committee found that nothing published by the paper had put British lives at risk](http://www.theguardian.com/world/2013/dec/03/guardian-not-intimidated-nsa-leaks-alan-rusbridger-surveillance). He also said that *The Guardian* had consulted government officials and intelligence agencies – including the FBI, GCHQ, the White House and the Cabinet Office – on more than 100 occasions before the publication of articles concerning Snowden’s information. He said that on only one occasion was there no consultation with the UK government before publication, when he feared an injunction could be sought to prevent publication (*The Guardian*, January 26, 2014, <http://www.theguardian.com/uk-news/2014/jan/26/d-notice-system-reviewed-edward-snowden>).

An official review of the DA Notice committee’s role, triggered by the Snowden affair, led in 2015 to its re-launch as the DSMA committee (and continuing dialogue over publication of Snowden revelations led to *The Guardian’s* deputy editor joining the committee as one of the media representatives). The review team, which included two former editors of national newspapers, criticised the ‘patchy engagement’ of some Government departments with the committee, and pointed out that in the USA contact about national security matters between the media and official sources ‘far exceed in depth and breadth those that exist in the UK’. The Government did not accept all the review team’s recommendations – for example, it rejected the idea that the committee should have an independent chair.

The outcome of the review was, in effect, that the DSMA committee will function in much the same way was the DA Notice committee did. The system remains, in essence, a voluntary code of media self-censorship on national security and defence issues. Advice is made available for the news media and book authors, through or facilitated by the DSMA-Notice committee secretariat, from the Government’s departments and its security and intelligence agencies, a major aim being to safeguard military and intelligence secrets, including the identities and operational whereabouts of the UK’s undercover agents and special forces, including those deployed against terrorists.

Editors who consult the DSMA-Notice committee secretariat sometimes decide to limit what is published in news and features, and sometimes feel able to publish information that they might otherwise leave out. But the committee has no statutory powers of enforcement. Editors do not have to seek advice or take the advice offered. An editor who publishes information of the type covered by a DSMA-Notice knows that the Government regards such information as sensitive, and therefore realises that there is a risk of prosecution if what is published is regarded as a breach of official secrets legislation.

There are books about the history of the Notice system: National Security and the D-Notice System, by Pauline Sadler (Dartmouth Publishing Co Ltd, 2001); Secrecy and the Media: The official History of the D-notice System, by Nicholas John Wilkinson (Routledge, 2009).

.

**Recap of major points**

■ Official secrets law is complex, and frequently controversial.

■ It protects national security and the safety of citizens, and can be used against foreign spies, terrorists, or other criminals.

■ But journalists say it is sometimes used to punish those who leak information which is politically embarrassing for the government, and to deter the media from revealing such information.

■ The law has wide definitions of what is secret. It has no public interest defence for anyone prosecuted for breaching it.

■ The DSMA-Notice system is a means by which the media can check if material they are considering publishing could be regarded as a breach of national security.

**Useful Websites**

**https://www.gov.uk/government/uploads/system/uploads/attachment\_data/file/346762/FOI201404093\_Official\_Secrets\_Act\_Form.pdf**

Official secrets form used by Ministry of Defence

**http://researchbriefings.parliament.uk/ResearchBriefing/Summary/CBP-7422**

House of Commons Library Briefing Paper ‘The Official Secrets Acts and Official Secrecy’

[**http://www.lawcom.gov.uk/app/uploads/2017/02/cp230\_protection\_of\_official\_data.pdf**](http://www.lawcom.gov.uk/app/uploads/2017/02/cp230_protection_of_official_data.pdf)

Law Commission’s ‘Protection of Official Data’ consultation paper 2017

**https://s3-eu-west-2.amazonaws.com/lawcom-prod-storage-11jsxou24uy7q/uploads/2017/02/cp230\_protection\_of\_official\_data\_summary.pdf**

Law Commission’s summary of its consultation paper

[**http://www.newsmediauk.org/write/MediaUploads/PDF%20Docs/NMA\_Response\_to\_Law\_Commission\_Consultation\_25\_July\_2017.pdf**](http://www.newsmediauk.org/write/MediaUploads/PDF%20Docs/NMA_Response_to_Law_Commission_Consultation_25_July_2017.pdf)

News Media Association’s response to Law Commission’s consultation

[**https://www.nuj.org.uk/news/nuj-calls-for-no-detrimental-changes-to-official-secrets-laws/**](https://www.nuj.org.uk/news/nuj-calls-for-no-detrimental-changes-to-official-secrets-laws/)

National Union of Journalists’ response to Law Commission’s consultation

[**https://infolawcentre.blogs.sas.ac.uk/files/2017/06/Law-Commission-Consultation-on-the-Protection-of-Official-Information-Woods-McNamara-Townend-09062017-final-online.pdf**](https://infolawcentre.blogs.sas.ac.uk/files/2017/06/Law-Commission-Consultation-on-the-Protection-of-Official-Information-Woods-McNamara-Townend-09062017-final-online.pdf)

Response by Professor Lorna Woods, Dr Lawrence McNamara and Dr Judith Townend to the Law Commission’s consultation

[**http://www.dsma.uk/**](http://www.dsma.uk/)

Defence and Security Media Advisory committee

[**https://www.ipco.org.uk/**](https://www.ipco.org.uk/)

Investigatory Powers Commissioner’s Office