Can you keep a secret? Legal and technological obstacles to protecting journalistic sources[1]

Richard Danbury, De Montfort University

Judith Townend, University of Sussex

Introduction

Journalists should protect their sources. They should, above all, protect those sources (including whistleblowers), that have provided them with information in confidence. This principle is included in journalistic codes of ethics around the world. It is a precept that is frequently interpreted rigidly, and at times so rigidly that it can put journalists in direct conflict with legal requirements to disclose information. Should a journalist comply with the law but break the ethical rule, the journalistic community will frequently condemn such an act.

In the United Kingdom, for example, the seventh principle of the National Union of Journalists' Code is that a journalist "[p]rotects the identity of sources who supply information in confidence and material gathered in the course of her/his work" (NUJ, 2011). In 2003, the NUJ expelled a young journalist for disclosing the identity of a source, even though he did so because that source had confessed to murder (Wallace, 2003). Similarly controversial was *The Times*' decision to obey a court order to assist police in their prosecution of former Liberal Democrat minister Chris Huhne. In 2012, Huhne was charged with perverting the course of justice in a speeding points case: the newspaper eventually provided the police with information that identified its informant, although the newspaper and the reporter defended their actions (Lewis, 2013). The prevailing assumption, then, is that journalists should protect a source that has been afforded confidentiality, whatever the personal and organisational cost.

This chapter considers whether this assumption is realistic. It surveys some of the contemporary legal and technological obstacles that journalists face in protecting their sources. It uses the United Kingdom as a case study, but similar concerns arise in other places in the world, as reflected by current discussions within the European Parliament (Lambert, 2017). Although the legal and technological obstacles are integrally connected, we will consider each category separately. The analysis is grounded in a round-table discussion that the authors organised at the University of London's Institute of Advanced Legal Studies in September 2016, with the support of Guardian News and Media, at which the issue of source protection in a digital age was discussed by 25 experienced investigative journalists, lawyers and representatives from NGOs (ILPC, 2017).

We conclude that, whatever a journalist's intentions, these obstacles now make protecting a source – their identity, and the confidential information they communicate – extremely difficult. In the Huhne case, for example, police used powers under the Regulation of Investigatory Powers Act 2000 to access mobile and landline phone records which identified the source used by a second newspaper (the *Mail on Sunday*). In doing so, they bypassed the need for judicial authorisation, and acted without the knowledge of the media organisation and journalist concerned (Craven, 2014). In such an environment, how can the NUJ's seventh principle – and other similar ethical rules – be maintained? Given the difficulties of protecting a source, what should a journalist do? In this chapter, we offer some legal, practical and technological suggestions.

The law: balancing interests

Before we demonstrate how source protection laws in the UK are becoming increasingly ineffective, it is first useful to consider briefly why laws of this type exist, and what they seek to do. The laws that

govern when, and under what circumstances, journalists can be compelled to reveal the identity of their sources arise from a need to balance competing societal interests. On the one hand, there are the interests of a source seeking anonymity because of the potential damage caused by the revelation of their identity; and the interests of a journalist seeking to protect his or her source, because this facilitates the flow of useful information provided by the source. On the other hand, there are the interests of the state in – for example - seeking information for the purposes of policing, national security or administrating justice.

It is appropriate to *balance* these interests because they are frequently instrumental interests, not absolute ones. There is no absolute value in protecting the identity of a journalists' source: sources are protected because this helps – amongst other things - journalists perform their 'watchdog' function. Such activity by journalists is necessary to a thriving democracy, as the European Court of Human Rights (amongst other international and national courts) has frequently recognised (see the discussion below). Equally, however, there is no absolute value in, for example, protecting national security in itself, or the administration of justice in itself. Society, we would argue, protects these interests appropriately only because they are instrumental in the protection of higher order interests – such as, for example, the right to life, the capacity of humans to flourish, or the imperative to treat individuals equally.

The fact that the societal interests commonly involved in source protection are frequently instrumental, not absolute, means they can be traded off against each other. Such trading off, however, needs to be predictable yet flexible, and normatively convincing. It is this that the laws that protect sources seek to achieve. It is a difficult task because it is difficult to formulate a set of rules with these qualities. But, generally speaking, this has been achieved over the past decades in the UK, and a relatively effective balance has evolved in response to the judgments of the European Court of Human Rights.

An example of balancing

A prominent example of this balance evolving over time can be seen in the application of the general statute that governs the protection of sources in UK law - the Contempt of Court Act 1981 (CCA, 1981). Section 10 CCA 1981 says that

"[n]o court may require a person to disclose, nor is any person guilty of contempt of court for refusing to disclose, the source of information contained in a publication for which he is responsible, unless it be established to the satisfaction of the court that disclosure is necessary in the interests of justice or national security or for the prevention of disorder or crime".

This, it can be seen, creates a basic rule that protects journalists' sources. It does this both by imposing a restriction on the ability of courts to order journalists to reveal their sources, but also by restricting the ability of the court to find a journalist, who is protecting their source, in contempt. The provision is wide in its range and application. For one thing, it does not only apply to journalists, because section 10 CCA 1981 is worded in such a way that bloggers and citizen journalists can use it: the section has been described as "indiscriminate in the ambit of its protection" (Blom-Cooper, 2008: 269).[2] For another, sources can be protected even where the information they communicate is of little value to society. In the words of a senior judge, Lord Justice Laws, concurring with the judgment of the rest of the Court of Appeal in a case in 2001:

> It is in my judgment of the first importance to recognise that the potential vice – the 'chilling effect' – of court orders requiring the disclosure of press sources is in no way lessened, and certainly not abrogated, simply because the case is one in which the information actually published is of no legitimate, objective public interest. Nor is it to the least degree lessened or abrogated by the fact (where it is so) that the source is a disloyal and greedy individual, prepared for money to betray his employer's

> confidences. The public interest in the non-disclosure of press sources is constant, whatever the merits of the particular publication, and the particular source. (*Ashworth Hospital Authority v Mirror Group Newspapers Ltd*, Court of Appeal, 2001: [101])

But, as part of the balancing of interests, what the section gives with one hand, it takes away with another. The protection afforded by the first phrase in section 10 is lessened by the provision's second phrase. One problem for those who wish to protect journalists and their sources is that this is also very wide. Consider, as an example, what may be 'in the interests of justice', and leave aside for present purposes the references in section 10 to national security, and the prevention of disorder or crime. It is likely, on the face value of these words at least, that it is in the *interests of justice* for a court to order a journalist to reveal the identity of a source, where that source has broken a duty of confidentiality. Duties of confidentiality will frequently be owed by sources to their employers, and a source will frequently breach such a duty by talking to a journalist. An employer who has had their confidentiality breached in such a way may well have a legal action against the source, and also the journalist.

Because both aspects of section 10 are wide, and competing interests are embodied in the provision, the courts have wrestled with how it should be applied. They have, to adopt the phrase used above, sought a balance that is predictable yet flexible, and normatively convincing. It has not been an easy process. A more complete survey of the evolution of the case law is beyond the scope of this chapter, and can be found elsewhere (for example, Cram 2009; Millar and Scott, 2016; Phillips, 2014), but one recurrent issue was that English law was frequently found to be out of kilter with European human rights law, in that it paid insufficient regard to the protection of sources (*Ashworth HA v MGN Ltd*, Court of Appeal: [97]; Nicol, 2009: 1.18).

This led to the UK courts aligning their interpretation of section 10 of the CCA, to the interpretation made by the European Court of Human Rights (ECtHR) of article 10 of the European Convention on Human Rights (ECHR) (see *Mersey Care v Akroyd (No2)* Court of Appeal, 2007). Article 10 protects freedom of expression.[3] This is engaged, because journalists employ their article 10 rights when communicating to the public, and an essential part of such communication can be that they receive information from sources. Being able to protect their sources helps maintain that flow of information. (Article 8,[4] the provision that protects privacy, can also be engaged, and this – as well as article 10 - will be discussed in more detail later.) The upshot of this is that section 10 CCA 1981, interpreted in the light of article 10, has evolved into a reasonably coherent and effective means of protecting sources, which balances such protection against other societal interests.[5]

But this protection is being undermined, and it is contemporary legal and technological change that has had this effect. Legal issues have arisen because there are other more specific laws that deal with particular instances where information is sought from journalists, and these can be less protective of journalistic sources than section 10 CCA 1981. Overuse, or inappropriate use of these laws, upsets the delicate balance. These laws can generally be divided into two categories – those that apply when individuals are seeking information from journalists, and those that apply when it is the state that is seeking information. The latter are more important for present purposes. Technological issues have arisen because of changes in communication technology, and in particular from data analytic techniques that can be applied to meta-data. We will discuss each in turn.

Upsetting the balance: legal issues

The statute of central importance to consider where the state is seeking information from a journalist is the Police and Criminal Evidence Act 1984 (PACE 1984). This established a regime that differentiates journalistic material from other information (s 13), which is further classified into either 'special procedure material' (s 14) or 'excluded material' (s 11), depending on whether it is held under a duty of confidence. If the authorities are seeking disclosure of special procedure material, the protections afforded to journalists are lesser, and it is easier to convince a court to order the release of

such material. The criteria that have to be applied – the 'access conditions' - can be found in schedule 1 to the Act. It is more difficult for the authorities to gain access to excluded material.

A senior media lawyer at our round-table said that protections under PACE 1984 for journalistic material – whether special procedure or excluded – have proved to be effective. Too effective in fact, in the opinion of some, and there have been suggestions that the protections that are afforded by PACE 1984 should be narrowed. Lord Justice Leveson, in his investigation into the culture, practice and ethics of the press in 2011-2012, explored this possibility, eventually recommending that the Home Office should consider amending specific protections contained within PACE (Leveson, 2012: 42; discussed, for example, in Phillips, 2014).

But this effective protection provided by PACE 1984 can already be reduced or evaded. One way this can happen is where another law provides a route by which the state can apply to the court to gain access to journalistic material, and this other route has weaker protections. There is a wide range of other laws that are available to the authorities for such a purpose. These include the Terrorism Act 2000 (section 37 and schedule 5, paragraph 5 and 6), the Criminal Justice Act 1987 (section 2), the Inquiries Act 2005 (section 21) and the Financial Services and Markets Act 2000 (section 13). Each of these statutes sets out the circumstances in which a state authority can obtain information, and they can overlap. This means that there can be multiple legal avenues through which the state can seek the same journalistic material.

It is here that our research indicated there can be a problem. Where, for example, the state is seeking journalistic material that deals with terrorism, the Terrorism Act 2000 applies. Access to material that is protected under PACE 1984 as special procedure material, and as excluded material, is gained much more easily under paragraphs 5 and 6 of Schedule 5 of the Terrorism Act 2000. A result of this is that the balance that attempts to protect conflicting societal interests has been disturbed. Participants at our roundtable reported that this a problem because the terrorism laws in question are very broadly framed, and that upsets the appropriate balance of competing societal interests described earlier in this chapter. (This point is also examined by Danbury in Chapter Two). Support for such a view can be found in the fact that the courts have decided that the police have used terrorism laws to gain access to journalistic material in situations where they should not have done so. (To be more precise, the Court of Appeal has found that the powers under schedule 7 of the Terrorism Act 2000 to stop and question people, if used in respect of journalistic information, is incompatible with the ECHR because it is not 'prescribed by law': *R (Miranda) v Home Secretary*. Court of Appeal, 2016: [94 – 117]). The net effect of this is that protections that should have been afforded to sources have been evaded. We have focused here on the example of terrorism and the Terrorism Act 2000, but other examples of this 'legislative arbitrage' could have been highlighted. It also results in the upsetting of a carefully balanced system in areas other than terrorism.

Upsetting the balance: technological issues

The second problem with the legal structures that protect sources, beyond this legislative arbitrage, results from technological innovation. It also arises because PACE 1984 focuses on protecting content, not the protection of sources and their identities as such. That this is a weakness can be demonstrated by considering the Regulation of Investigatory Powers Act 2000 (RIPA 2000), and how the police have used this act to seek journalistic information. RIPA 2000, until recently, provided the main legal framework governing the acquisition and disclosure of content and communications data. It has been supplemented and replaced in many areas by the Investigatory Powers Act 2016 (IPA 2016). But it is worth considering here, because there has been extensive experience of how it operates in practice. This experience not only illustrates the point we wish to make, but also offers a guide to some of the potential weaknesses of the IPA 2016. It also helps inform our suggestion of how these can be ameliorated.

RIPA 2000 enables intelligence and security agencies, police, customs and other public agencies to access communications data from telecoms companies for a variety of purposes. Part I chapter I allows for the interception of communications –in other words, the content. Part I chapter II allows for access to communications data through service providers. Part II creates (amongst other things) an authorisation defence for covert surveillance by public authorities (this includes following targeted people, and filming in public places). Intrusive surveillance (placing probes in houses or cars, and similar activities) requires prior judicial authorisation, and is only available for the investigation of serious crime, which the Act defines. State interference with property, such as planting a bug or installing wireless telegraphy, is dealt with by Part III of the Police Act 1997.

There is no specific mention made or protection in RIPA 2000 itself for confidential journalistic material, which may immediately seem to be a problem. This was, however, addressed by the *Acquisition and Disclosure of Communications Data Code of Practice*, a document that became effective from 25 March 2015. The Code introduced 'enhanced safeguards' to protect the article 10 ECHR rights of journalists (Home Office, 2015: 3.78 and 3.79). Effectively, this provided that where confidential journalistic material was likely to be obtained, the processes under PACE 1984 should be used. That meant that prior judicial approval would normally be required.

However, and this is the point, it subsequently became apparent that a number of police forces had used the communications data route under Part I chapter II of RIPA 2000, and applied directly to telecommunications companies for source-related data. In doing so, they had effectively circumvented the protections of PACE 1984 (see, for example, *News Group Newspapers v Metropolitan Police Commissioner* UK Investigatory Powers Tribunal, 2015). Indeed, in February 2015, the Interception of Communications Commissioner Sir Anthony May found the Code to be deficient. He recommended that it be altered, to "provide adequate safeguards to protect journalistic sources" (Interception of Communications Commissioner's Office, 2015: 37). Consequently, a revised *Code of Practice for the Interception of Communications Data* was issued in January 2016 (Home Office, 2016).

This highlights the weakness of PACE 1984 from the point of view of journalistic source protection. Meta-data – information about communication, rather than the contents of the communication itself – can be used by the authorities to identify journalistic sources. This can happen when information about who spoke to whom, on what machine, and on which account and when, is cross-referenced with other information. Moreover, more sophisticated data analytic techniques can be applied to reveal even more sensitive information. This is true in areas beyond journalistic source protection. A striking and disturbing example of such techniques being used in the 2016 American Election is described by Grassegger and Krogerus (2017.) Yet this meta-data is obtained more easily by authorities under RIPA 2000 than PACE 1984, and that means that authorities can evade the carefully balanced protections afforded by PACE 1984.

Here, we have just considered the UK, and in particular the provisions under PACE 1984 and RIPA 2000, but it is clear that this problem is likely to be more widespread. For one thing, it is likely to affect the implementation of the new IPA 2017, and measures of similar ambit – for example, the Digital Economy Bill, currently being considered by Parliament. It will also be relevant in other countries. As the academic lawyer Andrew Scott explained at the workshop that forms the basis of this chapter (ILPC, 2017), "[l]egal protection against disclosure/delivery up orders [is] irrelevant if surveillance, retention of/access to communications data, or interception of communications allows investigating authorities an easy route to information". Under such circumstances, it is very difficult – if not impossible – for a journalist to protect the anonymity of their sources. The answer to the question posed at the beginning of the chapter – can you keep a secret? – is, from a legal point of view, 'frequently no'.

Practical legal responses

What to do?[6] Legally, one way of redressing the balance is to look to the European Court of Human Rights. As has been described, the decisions of the ECHR on article 10 has deeply influenced decisions of domestic courts on section 10 CCA 1981, and it also influences (amongst other things) court interpretations of other laws that relate to source protection. This is because the UK has signed up to the European Convention on Human Rights, and incorporated the Convention into UK law by the Human Rights Act 1998. Section 3 of the HRA 1998 says that UK courts must interpret domestic legislation in a way that is compatible with the Convention, and section 6 indicates that courts themselves must act in ways that are compliant with the Convention.

There are two main articles in the ECHR that are relevant - article 10, already mentioned, which protects rights of free speech, and has special application to watch-dog journalism (see, for example, Millar and Scott, 2016; Nicolaou, 2012; Phillips, 2014 and the case law following *Goodwin v The United Kingdom* European Court of Human Rights, 1996), and article 8, which protects rights to privacy. These provide a standard against which contemporary laws, and the application of them, should be judged. It provides a way of assessing whether the balance between the competing societal interests, laid out earlier in this chapter, is achieved.

Article 10

As indicated above, article 10 protects freedom of speech. The leading ECtHR case on article 10 relating to source protection in this context is *Goodwin* (1996). In this case the Strasbourg Court found, amongst other things, that:

> protection of journalistic sources is one of the basic conditions for press freedom… without such protection, sources may be deterred from assisting the press in informing the public on matters of public interest… the vital public-watchdog role of the press may be undermined and the ability of the press to provide accurate and reliable information may be adversely affected… such a measure cannot be compatible with Article 10 of the Convention unless it is justified by an overriding requirement in the public interest.

The jurisprudence of the court has laid out a series of tests against which specific laws on source protection should be judged. These are based around the ECHR's three-fold test, that to be permissible, any infringement of article 10 should be prescribed by law, pursuant to a legitimate aim, and necessary in a democratic society – which includes a requirement that it should be proportionate. This means in *substantive* terms that any law – or its interpretation by the courts – needs to embody a variety of factors. These include the need to limit any interference with freedom of speech; to balance the public interests at stake between the dissemination of the source's information and the public interest in revealing their identity (or other relevant information); and the motives, objectives, and conduct of any journalist and their source.

The court also sets out some *procedural* factors that need to be built in to any law. These derive significantly from the case of *Sanoma Uitgevers BV v The Netherlands* (European Court of Human Rights, 2010), and include the requirement that any law that interferes with article 10 in relation to source protection must have effective legal procedural guarantees for a journalist. In practical terms, this means that there must be the guarantee of review by a judge or other independent and impartial decision-making body, of a decision that results in the revelation of a source's identity. Importantly, any review of such a decision must be made *in advance* of access to the information sought. Such a view was reinforced by the decision of *Telegraaf Media v The Netherlands*, European Court of Human Rights, 2012).

Article 8

As well as article 10, the other jurisprudence of the ECtHR that is relevant relates to article 8 – the right to a private life. Both the privacy of a journalist and their source can be interfered with when the state seeks to identify a journalist's source. Moreover, article 8 and article 10 can combine together where state surveillance is undertaken specifically to identify sources. (This is not always the case, and does not occur, for example, where the procurement of journalistic information is incidental to the purposes of an investigation).

Early guidance from the European court on how to apply article 8 came in *Klass v Germany* (European Court of Human Rights, 1978). This case confirmed the view that state interception or surveillance could be legitimate under article 8(2), but only where it is in accordance with the law, necessary in a democratic society, and proportionate (the usual test that the ECtHR applies). In interpreting this, the court noted that where the state is acting covertly, the individual will necessarily be prevented from seeking an effective remedy of his or her own accord, or from taking a direct part in any review proceedings. This is because such a person will not know that he or she is under surveillance, and will not know that there are any review proceedings in which they can take part. That means that, for any interception or surveillance to be compliant with article 8, the supervision of state powers in this context must be adequate to compensate for the absence of court oversight. In particular, the court subsequently explained in *Telegraaf Media*, this means that any review must take place before, rather than after covert interception or surveillance. This is because, a "review post factum… cannot restore the confidentiality of journalistic sources once it is destroyed" (*Telegraaf Media*, [101]).

Implications for source protection laws

What do these considerations mean for any evaluation of the law of source protection in the UK? They set out minimum standards, against which laws that seek to afford access to journalistic sources should be judged. They mean, for example, that the recently passed IPA 2016 needs to be applied in such a way that it sufficiently protects journalists' sources, and provisions on disclosure of public authority information in the Digital Economy Bill ought to be drafted with such protection built-in. In respect of the IPA 2016, we recommend that this can be achieved by the drafting and adoption of Codes of Practice in ways that comply with the ECtHR's jurisprudence, although we are concerned by the lack of an obligation to notify media parties of judicial authorisation requests in the legislation itself. In particular, such Codes should ensure that there is independent and impartial – and as far as can be achieved, transparent - oversight of any investigation that may reveal a journalist's sources. Where it is proposed that there should be surveillance for the purposes of identifying a source, this oversight ought to take place before any surveillance is undertaken. And, more generally, the Code should also be alive to, and prohibit, the abuse – or over-use – by the authorities of laws that permit access to meta-data and data analytics, to reveal journalistic information that is otherwise protected by law.

Nonetheless, we recognise that this may not be sufficient. A practical obstacle still stands in the way of ensuring these minimum standards in law. As Tom Hickman has argued cogently on the limitations of public law, judicial review is beyond the capability of most people (Hickman, 2017). If protection is only afforded to the rich, it cannot be fair and efficient protection. The point can be extended to the difficulty of bringing other types of legal challenges too: the costs and complexity of mounting a defence or challenging a court order are often prohibitive, especially to individuals and small media organisations.

Technology

This chapter has thus far concentrated on the legal risks to sources and journalists, and has discussed technological change in that context. However, rapid technological development in the 20th and 21st Centuries has had an impact on source protection beyond the law. It is to this that we now turn. The

appearance and widespread use of digital communication technologies, including internet based services, have been great enablers for freedom of expression – an individual wishing to reach a large audience no longer needs the financial resource to buy a printing press.[7] At the same time, however, digital communication methods have also allowed increased state and corporate capacity for surveillance. The technological protections for sources have not kept pace with the ability of states and other actors to use technology to intercept or monitor communications. Increasingly, journalists have become aware that any digital or other direct contact with a source who wishes to remain anonymous can make keeping a promise of confidentiality very difficult (see, for example, Posetti, 2015; Pearson, 2015). These difficulties have been brought into stark focus during contemporary debates about surveillance in the UK. Journalistic sources, and journalists, are increasingly vulnerable to being identified by state agencies and other actors.

Practical responses

However, technology – as well as presenting challenges for those who wish to protect their sources – also offers opportunities. There are a number of potential technological tools available to facilitate the protection of sources, and anonymous whistleblowing. A full survey of these is, again, beyond the scope of this chapter, but recommended resources can be found elsewhere (see Carlo and Kamphuis, 2016). Suffice to say for present purposes, that the resources available to journalists and their sources include tools such as SecureDrop, the secure deletion of information, the encryption of communication, and the encryption of internet browsing. These afford a response to the legal and technological difficulties that make it difficult for journalists to protect their sources.

Yet, at our meeting, practitioner journalists raised concerns about how these tools work in practice. For example, in respect of secure online submission systems, it was said that use of these was tricky to achieve without leaving digital footprints. These footprints can lead to the revelation of the identity of a source. Moreover, the difficulties in avoiding or minimising such a trail are enhanced where inexperienced or vulnerable sources are communicating with journalists, or where communication takes place through an intermediary. Even in situations where this is not the case, participants noted that jigsaw identification of sources via several pieces of information was a possibility. These, it was said, are not resolved by secure online deposit box technology.

Moreover, there are problems that arise from the very nature of anonymous secure online deposit systems. Anonymity is clearly one way of protecting source identity, and can be built into such tools. However, anonymity raises problems of its own. It makes it impossible, or very difficult, to assess the motivations and provenance of material provided to journalists. That means it is difficult for a responsible investigative journalist to use the material delivered by them, because they cannot be sure of its provenance, veracity, context, and the motive of the source. Knowledge of such information can be crucial in an evaluation of whether it is in the public interest to investigate and report. That said, it was observed that there might be other tools that could be used to overcome this difficulty, and OnionShare, an anonymous and secure filesharing tool, was mentioned as one.

Turning to secure means of communication, there are valuable tools available, such as the encryption programmes Pretty Good Privacy (PGP) and GNU Privacy Guard (GPG). PGP was essential to Glenn Greenwald's reporting of the Snowden revelations. However, the appropriateness of information security methods will vary in different circumstances, and not least because even the experts can find it difficult to use them correctly. Indeed, Glenn Greenwald very nearly missed his scoop, because he did not use encryption. In the words of Micah Lee, security engineer and journalist at *the Intercept*: "Greenwald didn't use encryption and didn't have the time to get up to speed, so Snowden moved on" after making initial anonymous contact with the journalist (Lee, 2014). Luckily for Greenwald, the story found him via another route, through the filmmaker Laura Poitras, who did use GPG.

But even this route was not easy. To get in touch with her initially, Snowden had first to contact Micah Lee, to obtain her GPG key. Moreover, Lee's account of his crucial role in the process exposes

the potential for source identification even with a source as technologically competent as Snowden. In his first email to Lee, Snowden (writing anonymously) had forgotten to attach his key, which meant that Lee could not encrypt his response. Therefore, Lee was forced to send him an unencrypted email requesting his key. Lee comments: "His oversight was of no security consequence - it didn't compromise his identity in any way - but it goes to show how an encryption system that requires users to take specific and frequent actions almost guarantees mistakes will be made, even by the best users" (Lee, 2014).

If it is difficult for professionals to protect themselves using these technical tools, it is even more difficult for non-professionals. A participant directly working with whistleblowers emphasised this point, when observing that many people do not think about encryption; sources with Edward Snowden's mindset and technical background are rare. For many sources, the main concern is going public; and when they are dealing with the media, to what extent they trust the journalist. Encryption, and similar ways of covering their digital tracks, is a secondary consideration for such people.

Given these opportunities to slip up, some of our participants wondered if old fashioned and pre-digital methods could still serve a purpose; for example, receiving information by post, fax or hand-delivery. Another suggested that reporters could advertise online when they will be in the office, so an individual could find them in person. While this could be useful in some situations, another participant - a freelance - observed that this would not necessarily help those journalists who operated without an office base. And, in any event, any contact between a source and a journalist could still be vulnerable to surveillance, by tracking smart phone locations, for example. In addition, as Smyth and O'Brien argue:

> the capability to tap your computer or phone has been decentralized and privatized… that power is potentially in the hands of a far wider group: people sharing [a] wireless network at a cybercafé can snoop on your instant messages… hackers can break into your email account; to minimise risks of state and private interference investigative journalists should always adopt appropriate data security protocols' (Committee to Protect Journalists, 2012: 17).

Risk assessment, in the end, will be essential, and this requires thinking about who the target of the information is, what resources are available to them, whether they have the motive to seek to identify a source, and whether they have the opportunity to do so. Thinking through this process is of central importance *before* any communication takes place. In practice of course, as the Snowden-Greenwald example shows, this is not always possible, and even when it is, it is not always the complete answer. Ultimately, therefore, we feel there is no technological solution to the threats to source protection for journalists. These are questions of human interaction, and the ideal protection of sources comes from the behaviour of sources and journalists. Technology is a tool: but more important than the tool, is the way it is used by human beings.

Conclusion

These legal and technological threats to the protection of anonymous sources' identity and communications return us to our original question. Given these legal and practical difficulties of protecting a source evident from both our discussions with practitioners and a review of the literature, what should a journalist do? In our report of February 2017 we make recommendations, divided into actions for different actors. We have mentioned some specific suggestions on current law and policy (namely, the Investigatory Powers Act and the Digital Economy Bill, passing through Parliament at the time of writing), that we feel should sufficiently protect journalists and their anonymous sources in ways that are compliant with the UK's international human rights obligation, particularly those under the ECHR. Essential to this is the provision of independent judicial oversight regimes to safeguard legitimate protection. Comparable points, though obviously transposed to different doctrinal contexts, can be made in other jurisdictions.

For journalists and news organisations, our recommendations also apply more broadly than the UK. We focus on the care journalists should show for sources, and suggest they and their organisations should review and strengthen policies on secure technology, source care and protection. We suggest that they consider how journalists engage with sources that wish to remain anonymous, and offer and participate in training on working with confidential sources to make journalists and sources aware of the practicalities and limitations of source care and protection. We also identify a number of research questions that need further study. It was evident from our discussion that we needed to draw on better empirical evidence on the extent to which different jurisdictions offer protection for whistleblowers and journalists, and whether lessons can be learned from legislation in other territories. It is clear that we need to interrogate definitions of journalism and evaluate whether this can help the drafting of source protection laws.

Against this background, we also see the need to re-visit international journalists' ethical codes. We feel there should be additional provisions for journalists to warn their sources of the vulnerabilities of their communication before offering assurances of anonymity. The Society of Professional Journalists in the United States, for example, says that anonymity should be reserved 'for sources who may face danger, retribution or other harm, and have information that cannot be obtained elsewhere' (Society of Professional Journalists, 2014). We feel this limitation – and similar limitations – is not enough, nor are the general provisions on harm avoidance sufficient. There is scope for ensuring that additional information about a source's vulnerability is provided before proceeding with the contact.

In sum, we conclude that a journalist should continue to strive for confidentiality, but need to be alert to the legal and technological dangers that might reveal their sources. They should consider when it would be appropriate to share their concerns with a source. Not all anonymous sources will anticipate the potential for interception as Edward Snowden did, or take such extreme steps to protect their identity. There may be an ethical obligation to inform them of their vulnerability before offering confidentiality and proceeding with the investigation. These obligations arise because it is very difficult for modern journalists truthfully to answer 'yes', when asked the question: 'can you keep a secret?'.

References

Blom-Cooper Louis. (2008) 'Press Freedom: a Constitutional Right or Cultural Assumption?' [2008] *Public Law* 260.

Breiner, James. (2014) 'What Freedom of the Press Means for Those Who Own One'. [online] MediaShift. Available at: <http://mediashift.org/2014/12/what-freedom-of-the-press-means-for-those-who-own-one/> [Accessed 12 Mar. 2017].

Carlo, Silke and Kamphuis, Arjen. (2016) *Information Security for Journalists*. 1.3 ed. [online] London: The Centre for Investigative Journalism. Available at: <http://www.tcij.org/resources/handbooks/infosec> [Accessed 20 Mar. 2017].

Committee to Protect Journalists. (2012) *CPJ Journalist Security Guide: Covering the News in a Dangerous and Changing World*. New York: CPJ

Contempt of Court Act 1981 (1981). London: The Stationery Office.

Court of Appeal (2001) *Ashworth Hospital Authority v Mirror Group Newspapers Ltd.* [2001] 1 WLR 515: CA.

Court of Appeal (2007). *Mersey Care v Akroyd (No2)*. 94 BMLR 84.

Court of Appeal, (2016) *R (Miranda) v Home Secretary*. [2016] EWCA Civ 6.

Cram, Ian. (2009) *Terror and the War on Dissent.* Dordrecht: Springer.

Craven, Nick. (2014) 'How police hacked the Mail on Sunday'. [online] Mail Online. Available at: <http://www.dailymail.co.uk/news/article-2780809/How-police-hacked-Mail-Sunday-Officers-used-anti-terror-laws-seize-phone-records-identify-source-exposed-Chris-Huhne-s-speeding-points-fraud.html> [Accessed 12 Mar. 2017].

Criminal Justice Act 1987 (1987). London: The Stationery Office.

European Convention on Human Rights, 1953. Rome: Council of Europe.

European Court of Human Rights. (2010) *Sanoma Uitgevers BV v The Netherlands*. (Application No. 38224/03 [2010] ECHR 38224/03.

European Court of Human Rights. (2012) *Telegraaf Media v The Netherlands*. (Application No. 39315/06 [2012] 34 BHRC 193.

European Court of Human Rights. (1996) *Goodwin v The United Kingdom.* (1996) 22 EHRR 12.

Financial Services and Markets Act 2000 (2000). London: The Stationery Office.

Grassegger, Hannes. and Krogerus Mikael. (2017) 'The Data that Turned the World Upside Down' [Online] Motherboard.vice.com. Available at:< https://motherboard.vice.com/en_us/article/big-data-cambridge-analytica-brexit-trump?utm_source=vicefbusads&utm_campaign=interest> [Accessed 21 Mar. 2017].

Hickman, Tom. (2017) 'Public Law's Disgrace'. *UK Constitutional Law Association*. [Online] Available at: <https://ukconstitutionallaw.org/2017/02/09/tom-hickman-public-laws-disgrace/> [Accessed 12 Mar. 2017].

Home Office. (2015). *Acquisition and Disclosure of Communications Data Code of Practice*.

Home Office. (2016) *Code of Practice for the Interception of Communications Data*.

Human Rights Act 1998. London: The Stationery Office.

ILPC (2017). 'Source protection report and resources'. *Information Law & Policy Centre blog*. [Online] Available at: <https://infolawcentre.blogs.sas.ac.uk/source-protection-report-2017/> [Accessed 12 Mar. 2017].

Inquiries Act 2005 (2005). London: The Stationery Office.

Interception of Communications Commissioner's Office. (2015) *IOCCO inquiry into the use of Chapter 2 of Part 1 of the Regulation of Investigatory Powers Act (RIPA) to identify journalistic sources*, 2015 [Online]. Available at: <http://iocco-uk.info/docs/IOCCO%20Communications%20Data%20Journalist%20Inquiry%20Report%204Feb15.pdf> [Accessed 17 Mar. 2017].

Investigatory Powers Act (2016). London: The Stationery Office.

Lambert, Jean. (2017) 'While the UK attacks whistleblowers, the EU is defending them – that is, until Brexit happens'. [Online] Independent.co.uk. Available at: <http://www.independent.co.uk/voices/brexit-eu-britain-whistleblowers-european-parliament-defending-them-a7589581.html> [Accessed 12 Mar. 2017].

Lee, Micah. (2014) 'Ed Snowden Taught Me To Smuggle Secrets Past Incredible Danger. Now I Teach You'. [online] The Intercept. Available at: <https://theintercept.com/2014/10/28/smuggling-snowden-secrets/> [Accessed 12 Mar. 2017].

Leveson, Brian. (2012) *An Inquiry into the Culture, Practices and Ethics of the Press: Executive Summary and Recommendations.* London: The Stationery Office.

Lewis, Helen. (2013) *Isabel Oakeshott: Vicky Pryce double-crossed me*. [online] The New Statesman. Available at: <http://www.newstatesman.com/staggers/2013/03/isabel-oakeshott-vicky-pryce-double-crossed-me> [Accessed 12 Mar. 2017].

Liebling, Abbot (1964) *The Press*. New York: Ballantine Books

Millar, Gavin. and Scott, Andrew. (2016) *Newsgathering: Law, Regulation, and the Public Interest*. Oxford, New York: Oxford University Press.

National Union of Jounralists, (2011). *NUJ Code of Conduct.* [Online] Available at: https://www.nuj.org.uk/about/nuj-code/ [Accessed 21 Mar.2017].

Nicol, Andrew; Millar, Gavin; and Sharland, Andrew (2009). *Media Law and Human Rights*. Oxford: Oxford University Press.

Nicolaou, George. (2012) *The Protection of Journalists' Sources*, in Casadevall J., Myjer E., O'Boyle, M., & Austin, A. (eds) *Freedom of Expression: Essays in Honour of Nicolas Bratza*, Oisterwijk: Wolf Legal Publishers.

Pearson, Mark. (2015) *How surveillance is wrecking journalist-source confidentiality*. [online] The Conversation. Available at: <http://theconversation.com/how-surveillance-is-wrecking-journalist-source-confidentiality-43228> [Accessed 12 Mar. 2017].

Phillips, Gillian. (2014). *On Protection of Journalistic Sources*. [online] Centre for Media Pluralism and Media Freedom. Available at: <http://journalism.cmpf.eui.eu/discussions/on-protection-of-journalistic-sources/> [Accessed 12 Mar. 2017].

Police Act 1997 (1997). London: The Stationery Office.

Police and Criminal Evidence Act 1984 (1984). London: The Stationery Office.

Posetti, Julie. (2015) 'Protecting Journalism Sources in the Digital Age' in Rachel Pollack Ichou (ed) *World Trends in Freedom of Expression and Media Development: Special Digital Focus*. Paris: UNESCO.

Regulation of Investigatory Powers Act 2000 (2000). London: The Stationery Office.

Society of Professional Journalists (2014), *SPJ Code of Ethics* [online]. Available at https://www.spj.org/ethicscode.asp [Accessed 11 April 2017]

Terrorism Act 2000 (2000). London: The Stationery Office.

Townend, Judith. and Danbury, Richard. (2017). *Protecting Sources and Whistleblowers in a Digital Age*. [Online] London: Institute of Advanced Legal Studies. Available at: <https://infolawcentre.blogs.sas.ac.uk/source-protection-report-2017/> [Accessed 12 Mar. 2017].

UK Investigatory Powers Tribunal (2015) *News Group Newspapers v Metropolitan Police Commissioner*. [2015] UKIPTrib 14_176-H.

Wallace, Ashleigh. 2003. 'Union kicks out journalist'. [online] BelfastTelegraph.co.uk. Available at: <http://www.belfasttelegraph.co.uk/imported/union-kicks-out-journalist-28154342.html> [Accessed 12 Mar. 2017].

[1]Material in this chapter is drawn from a research project undertaken by the authors in autumn 2016 at the Institute of Advanced Legal Studies with the support of Guardian News and Media, and published as a working report (Townend and Danbury, 2017). The authors offer their thanks to all who contributed to this initiative and in particular, Dr Andrew Scott (LSE) and Gillian Phillips (The *Guardian*) for their assistance with building an overview of the relevant law. Of course, all errors and commissions remain the authors' own.

[2] It is important to note a point that follows from this. In this chapter we discuss the issue of *journalistic* source protection, and protecting *journalists'* sources. However, we do not necessarily mean to confine the arguments we advance to institutional journalists. They can apply to what can be called functional journalists too – those undertaking journalistic activity, without being members of an institution of journalism. Whether they do or not is a complex and important area, but depends on a discussion beyond the scope of this chapter. We touch on it briefly in the conclusion.

[3] 1) Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This Article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises. (2) The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary.

[4] 1) Everyone has the right to respect for his private and family life, his home and his correspondence. (2) There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

[5] Although it is not perfect. A significant problem, which we return to at the end of this chapter, results from the transaction costs involved in defending a legal action that seeks a source, and the chill those costs entail. It may well be cheaper and easier for a journalist or a journalistic organisation – particularly smaller operations and freelances – to release source related information that is requested of them by a lower court, than to appeal such an order.

[6] This section derives from Dr Andrew Scott's presentation at the ILPC workshop (ILPC, 2017).

[7] In 1960 AJ Liebling famously noted that "Freedom of the press is guaranteed only to those who own one" (Liebling, 1964; and see Breiner, 2014).