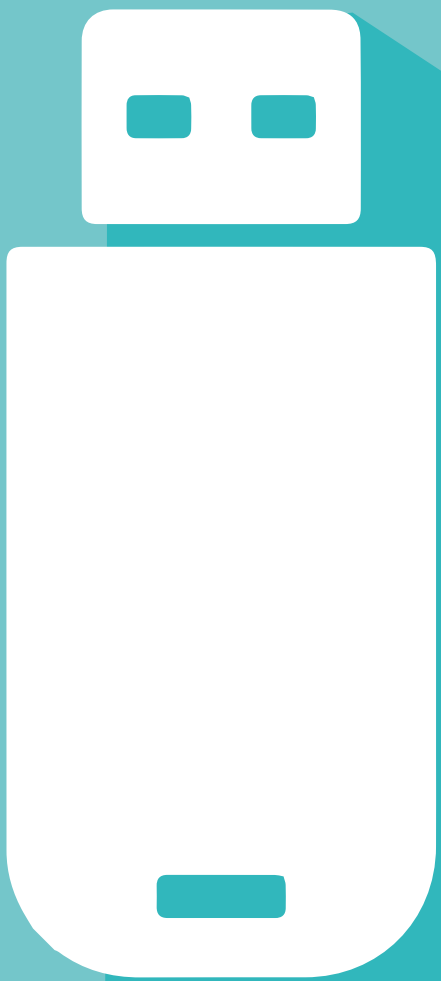
Information Law and Policy Centre, Institute of Advanced Legal Studies:
An initiative supported by Guardian News and Media

Protecting Sources and Whistleblowers in a Digital Age



IALS INSTITUTE OF ADVANCED LEGAL STUDIES | SCHOOL OF ADVANCED STUDY UNIVERSITY OF LONDON

Foreword

Developments in digital technology open up vast opportunities for news organisations to create and distribute journalism in new ways. The process of journalistic investigation has changed too. The laptop and phone play as important a role in the life of an investigative reporter as the notebook once did.

Contact with a source is now as likely to happen digitally as in person. We create vast tracts of data - from internet connection records to communications data – and this information can tell interested parties everything about a reporter, the story they're pursuing, and the source they're protecting.

But, while the process may have changed, we still tell the same kinds of stories: scrutinising those in power; exposing wrongdoing; and working in the public interest. Our journalism continues to rely on an ability to offer protection and anonymity for sources and whistleblowers. Evidence from sources lay behind our reporting of tax transgressions in the Panama Papers and behind enabling ex-footballers to tell their stories of abuse in the sports youth system.

I'm delighted that the Guardian has supported the Institute of Advanced Legal Studies in analysing how technological advances expose journalists and their sources to interference by state actors, corporate entities or individuals.

As this report sets out, it is imperative that we all continue to call on those in power to improve our legal framework on a number of fronts. At a time when journalistic protections are more important than ever, the UK Parliament has just passed an act that brings in one of the most draconian surveillance regimes anywhere in the world, with the Investigatory Powers Act. It enables law enforcement and agencies to access journalists' data without the journalist ever knowing.

As we continue to press for more protections from policymakers, we must also do everything we can to help ourselves, embracing a new age of technology with care. Alongside our sources, we must continue to uncover the truth.

Katharine Viner
Editor-in-chief, Guardian News and Media

Summary

This brief reports on a research initiative on confidential source and whistleblower protection led by researchers at the Information Law and Policy Centre at the Institute of Advanced Legal Studies. It includes the findings of discussions with a specialist group of 25 investigative journalists, representatives from relevant NGOs and media organisations, media lawyers and specialist researchers in September 2016.

Main findings

- The UK Government has, in recent years, pursued a number of policies and legislative proposals that have substantially weakened protections for sources. Most urgently, these include the Investigatory Powers Act that has recently become law and the Digital Economy Bill currently being considered by Parliament.
- Technological change means that journalists, freelancers and publications are faced with previously unprecedented difficulties in protecting their sources. 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.
- Although a number of domestic and European legal protections exist for the protection of confidential sources, their effectiveness is considerably weakened by technology that provides an easy route to information; and the use of covert powers to which journalists and sources may be oblivious.
- Working investigative journalists and media lawyers, many with several decades of experience, are profoundly concerned about the growing technological and legal vulnerability of confidential sources including whistleblowers, the protection of whom is essential to the pursuit of responsible journalism in the public interest.
- There is a need to strengthen whistleblower protection legislation in the UK.

25 investigative journalists, representatives from relevant NGOs and media organisations, media lawyers and specialist researchers

Summary of 10 recommendations

We recommend that policymakers and lawmakers:

1 Guarantee that the Investigatory Powers Act Codes of Practice sufficiently protect journalists and their anonymous sources, in ways compliant with the UK's international human rights obligations.

2 Make certain that the judicial oversight regimes are designed and operate in way that sufficiently protects journalists and their anonymous sources.

3 Ensure that Part V of the Digital Economy Bill is amended, so that it does not criminalise appropriate disclosures by whistleblowers operating in the public interest.[1]

We recommend that journalists and news organisations:

4 Review and strengthen policies on secure technology, source care and protection.

5 Review how journalists engage with sources that wish to remain anonymous.

6 Offer or seek training on working with confidential sources to make journalists and sources aware of the practicalities and limitations of source care and protection.

We recommend that researchers and NGOs:

7 Examine the merits of extending public interest defences for whistleblowers.

8 Analyse and see what can be learnt from whistleblowing legislation in other territories.

9 Seek adequate definitions of journalism and journalists, and evaluate whether this can help the drafting of source protection laws.

10 Produce a public log of cases where source protection is breached, and in what ways.

Future plans

The authors of this report propose to:

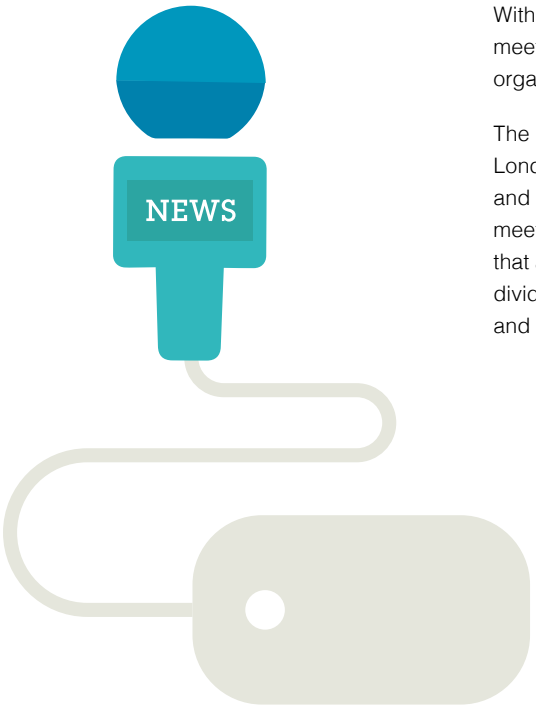
- Set up a mailing list for the group which convened to produce this report, to enable a rapid and well informed response to policy developments.
- Explore the possibility of future research and research impact funding to build on the findings of this meeting and other relevant projects.
- Undertake further empirical research and provide periodic updates on the severity of the threat to source protection in 2017.
- Encourage the formation of an all-party group in Parliament which would have the capacity to highlight and examine issues of source protection and related threats to public interest journalism.
- Add further resources to a project website page, where this report will be published.

Background

It is well established that a journalist has a moral imperative to protect confidential sources. This is a principle that is explicitly stated in the National Union of Journalists code of conduct. But achieving this has not always been easy. Recent technological developments have exacerbated these difficulties. 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; it may not be practically possible given the technical tools and legal powers available to police and other authorities.[2] 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.

There is another side to this coin: it has always been difficult for concerned individuals to report wrongdoing – whether to journalists or to others – from within organisations without attracting unfair retribution. Digital communication technology increases these difficulties, should the whistleblower want to communicate their concerns anonymously or confidentially to a journalist.

This is a multifaceted issue. There are a number of different types of risk that arise, and a range of different people who bear these risks. Legally, there are a variety of domestic and international laws that affect the position of contemporary whistleblowers, journalists, not-for-profit campaigners and other individuals working to expose information in the public interest and to hold those with political, economic and commercial power to account. Moreover, it must be recognised that another facet of the issue is that not all journalistic outputs may be considered to be in the public interest when taken in isolation.



Within this context, researchers at the Information Law and Policy Centre[3] convened a meeting of 25 investigative journalists, representatives from relevant NGOs and media organisations, media lawyers and specialist researchers.

The meeting on 16th September 2016 was held at the Institute of Advanced Legal Studies in London under Chatham House Rules, with the support of the policy team at Guardian News and Media. This brief summarises the main points made by different participants at the meeting, and in light of the views expressed the authors offer recommendations for changes that are deemed necessary to assist the protection of sources in digital environments. It is divided into four sections: the legal framework, practical considerations, technological factors, and possible initiatives.

[2] See, for example, Mark Pearson (2015): http://theconversation.com/how-surveillance-is-wrecking-journalist-source-confidentiality-43228. [3] http://bit.ly/infolawpolicy.

The legal framework for source protection

Before the workshop, those who participated were directed to the overview of the law written by Gillian Phillips, head of editorial legal at The Guardian, which she had prepared for the European University Institute.[4] This was supplemented by a more detailed account, which was provided orally at the meeting by Gillian Phillips and Andrew Scott, Associate Professor in Law at the London School of Economics and co-author of Newsgathering: Law, Regulation, and the Public Interest (OUP, 2016).

The account at the meeting started by identifying the core statement of principle on source protection set out in section 10 of the Contempt of Court Act 1981 (CCA 1981). This installs a default, although qualified, rule that journalists' sources and materials will be protected as a matter of law. (The complementary statute relevant to considerations of the protection of individuals who disclose public interest information (whistleblowers) is the Public Interest Disclosure Act 1998 – PIDA 1998). Section 10 CCA 1981 was – arguably at least – an advance on the common law that came before it. But in practical legal terms, it has by now been subsumed within article 10 of the European Convention on Human Rights (ECHR), which guarantees freedom of speech. This, of course, has been incorporated into English law by the Human Rights Act 1998.

The leading case on article 10 in this context is *Goodwin v UK*.[5] This holds, 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'.

However, these words have been honoured more in the breach, rather than in the observance, in UK case law, as the European Court of Human Rights (ECtHR) have repeatedly found that British judges are all too ready to afford access to journalistic sources.

The legal bases on which British judges afford such access varies. Different laws are relevant, depending on whether it is the state that is seeking information from a journalist, or whether the information is being sought by private individuals. Perhaps the most significant for private individuals is the power the court has to make *Norwich Pharmacal orders*.[6] When granted, these place a journalist (or any other party mixed up in the tortious act of others) under a duty to assist, by providing information – including the identification of an alleged wrongdoer – to a claimant.[7] A claimant can, therefore, ask a court to use this power to disclose the identity of a source, where it is asserted that the source has – for example – broken the duty of confidence he or she owes to the claimant, by providing a journalist with information. According to a participant with expertise in this area, there had not been any cases where the rights of the individual to disclose the information under PIDA have been expressly tested as against these powers.

[4] http://bit.ly/sourceprotection. [5] (1996) 22 EHRR 123. [6] *Norwich Pharmacal co v Customs & Excise Commissioners* [1974] AC 133. [7] See, for example, *The Rugby Football Union v Consolidated Information Services Limited* (formerly Viagogo Limited) [2012] UKSC 55.

Where it is the state that is seeking information, some of the most important laws include the Police and Criminal Evidence Act 1984 (PACE, ss 9, 11, 13, 14 and sch 1), the Terrorism Act 2000 (TA, s 37 and sch 5, para 5 and 6), the Criminal Justice Act 1987 (s 2), the Inquiries Act 2005 (s 21) and the Financial Services and Markets Act 2000 (s 13). Each of these statutes sets out the circumstances in, and the purposes for, which a state authority can obtain information. This is not a comprehensive list.

PACE focuses on protecting content: there is no absolute protection for sources under UK law. Nevertheless, the protection under PACE for excluded (i.e. confidential) source material is reasonably strong, and, while PACE safeguards for 'special procedure' material are weaker, they were said to work.

The structures created by these acts are an attempt to balance competing interests, namely those of the sources seeking anonymity, a journalist seeking to protect the source, and the legitimate interests of the state in seeking information for the purposes of policing, and administrating justice. For example, the Police and Criminal Evidence Act 1984 (PACE) includes rules for accessing journalistic material, i.e. content. It differentiates journalistic material from other information and classifies it as 'special procedure material' or 'excluded material' depending on whether it is held under a duty of confidence. Schedule 1 provides access criteria for special procedure material. Excluded material cannot normally be accessed under PACE (para 3 of sch 1 comprises a savings clause for earlier legislation under which excluded material could be obtained, for example the Official Secrets Act 1920). Such journalistic material may also be acquired via terrorism-related legislation such as the Terrorism Act 2000, which provides for access to both categories of information. Both PACE and the TA contain 'access conditions' including whether the material would be in the public interest to disclose, but judicial discretion is also relevant and ECHR Article 10 can be taken into account.

PACE focuses on protecting content: there is no absolute protection for sources under UK law. Nevertheless, the protection under PACE for excluded (i.e. confidential) source material is reasonably strong, and, while PACE safeguards for 'special procedure' material are weaker, they were said to work. The protections from disclosure where the Terrorism Act bites, however, are weaker still. What is important, though, is that even these qualified protections have been undermined in contemporary times, and concerns about the ability to protect journalistic sources from the state are becoming more acute. This is because, as will be seen from the subsequent discussion, these delicate balances risk being crushed by contemporary technological and legal developments.

In practice, the rulings of the ECtHR combined with domestic law, provide a list of substantive and procedural factors that need to be taken into account by a court, when deciding whether to permit disclosure of a journalists' source. The substantive factors include:

- the extent of the proposed interference with freedom of speech
- general and particular public interests at stake in dissemination of the sources' information to the public
- objectives said to justify disclosure
- the motive and conduct of source
- the journalist's conduct
- whether confidentiality was expressly promised to the source
- other rights of the journalists, sources and third parties.

The procedural factors, arising significantly from the ECtHR case of *Sanoma Uitgevers BV v The Netherlands, include:*[8]

- the measure in issue should have some basis in domestic law
- there must have been effective legal procedural guarantees for the journalist
  - the first and foremost of these is the guarantee of review by a judge or other independent and impartial decision making body
  - any review must be in advance of access to the information sought. In *Sanoma*, the ECtHR said that a subsequent review would 'undermine the very essence of the right to confidentiality'. Such a view was reinforced in the case of *Telegraaf Media v The Netherlands*[9]
- the action must be necessary for the attainment of the specified purpose
  - such a purpose must be specific and clearly identified
  - the applicant must produce evidence of the importance of the objective being pursued, and how that will be advanced by disclosure
  - there must be no alternative means by which the purpose for which disclosure is sought might be achieved.

There was then a more detailed discussion of some specific UK powers, and the extent to which they were compliant with article 10. Attention was paid to the Regulation of Investigatory Powers Act 2000 (RIPA 2000), which at the time of the meeting provided the main UK legal framework governing the acquisition and disclosure of content and communications data. RIPA 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 - i.e. content. Part I chapter II allows for access to communications data through service providers[10] and Part II creates (amongst other things) an authorisation defence for covert surveillance by public authorities (following, filming etc. in public places). Intrusive surveillance (probes in houses or cars etc.) requires prior judicial authorisation, and is only available for the investigation of serious (as defined) crime. Part III of the Police Act 1997 deals with state interference with property, such as planting a bug or installing wireless telegraphy.

There is no specific mention made or protection in RIPA itself for confidential journalistic material. A new Acquisition and Disclosure of Communications Data Code of Practice under RIPA became effective from 25 March 2015 and introduced 'enhanced safeguards' to protect the Article 10 rights of journalists.[11] Effectively, this provides that where confidential journalistic material is likely to be obtained, processes under PACE should be used, so that prior judicial approval is normally required. However, it subsequently became apparent that a number of police forces had used the communications data route under RIPA to go directly to telecommunications companies for source-related data, thereby effectively circumventing the PACE protections.

[8] Application No. 38224/03 [2010] ECHR 38224/03. [9] Application No. 39315/06 [2012] 34 BHRC 193. [10] This was the subject of a case at the Investigatory Powers Tribunal, brought by Tom Newton Dunn, Anthony France and Craig Woodhouse: *News Group Newspapers Ltd and others v Commissioner of Police for the Metropolis* [2015] UKIPTrib 14/176/H. [11] Paras 3.78 to 3.84.

Indeed, in February 2015, the Interception of Communications Commissioner Sir Anthony May found that the then current Home Office rules for using RIPA did not 'provide adequate safeguards to protect journalistic sources'. Consequently, a revised Code of Practice for the Interception of Communications Data was issued in January 2016.[12]

As well as article 10, the jurisprudence of the ECtHR on article 8 – the right to a private life – is relevant, and was discussed. A central early case was identified as *Klass v Germany*.[13] The case confirmed that state interception or surveillance, under article 8(2), could be legitimate if it is in accordance with the law, necessary in a democratic society, and proportionate. But the court noted that 'the individual will necessarily be prevented from seeking an effective remedy of his own accord or from taking a direct part in any review proceedings'. 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 this absence of individual oversight through the courts.

This case, and other jurisprudence of the European Court, meant that legislation was required to ensure that UK law complied with article 8 of the ECHR. As with the general powers of the security services and special police powers, the use of interception and surveillance powers could not be left without a statutory basis in the UK. Such legislation included the Interception of Communications Act 1985, the Security Service Act 1989, Part III of the Police Act 1997, and – indeed – the RIPA 2000 itself.

Furthermore, specific principles can be garnered from the ECtHR jurisprudence about the nature of this legislation, and what it must contain to comply with article 8:

- legislation authorising surveillance must be clearly and carefully drafted
- surveillance must be reviewed and accompanied by procedures guaranteeing rights
- it is desirable for a judge to supervise any relevant process, although other safeguards might suffice, provided those supervising are independent and can exercise effective and continuous control
- outside the most exceptional circumstances, public authorities must obtain authorisation in advance to undertake surveillance.

Article 8 and article 10 of the ECHR can combine together, and set standards that the ECtHR indicates should apply where state surveillance is undertaken specifically to identify sources. (This is not the case where the obtaining of journalistic information is incidental to other investigatory purposes.) Where this happens, and where surveillance is undertaken for such a purpose, the case of *Telegraaf Media* (as mentioned above) emphasises that a 'review post factum… cannot restore the confidentiality of journalistic sources once it is destroyed'.[14]

[12] https://www.gov.uk/government/publications/interception-of-communications-code-of-practice-2016. [13] Application No. 5029/71 [1978] ECHR 4, (1980) 2 EHRR 214. [14] Application No. 39315/06 [2012] 34 BHRC 193.

Concerns arising from the legal framework

The investigative journalists, media lawyers and representatives of whistleblowers who were present raised a number of concerns about the law.

A general, overriding concern was that technology might have made some, many or even all of these legal protections for journalists and their sources redundant. This is because legal protection against disclosure and delivery up orders are irrelevant if surveillance, retention of and access to communications data, or interception of communications allows investigating authorities an easy route to information.

Moreover, legal protections may have become ineffective – if ever they were effective. This is because if covert powers are used, a journalist and source will not know this has occurred – intrusion may become apparent only if the material is used in legal proceedings (this is the point that was recognised in Klass.) In this scenario, the only protection can be a legal requirement that decision-makers properly weigh source/journalist Convention rights against any legitimate aims of investigation. It is very important indeed that they do so. Concerns about the Investigatory Powers Bill (IP Bill, since passed as the Investigatory Powers Act), set out by Guardian News and Media in a briefing earlier this year, included the fact that it does not allow for any prior notice to be given to media organisations, and that it does not provide the judicial commissioners making decisions on access to journalistic material with the power to request information from a news organisation when they require more information.

It was noted that examples of states using covert powers against journalists without journalists' knowledge were easy to find. They include targeted hacking of journalists' email in China;[15] the NSA targeting of journalists' records;[16] the US Attorney General's obtaining of phone records of AP journalists in 2013,[17] the police's surveillance of the local newspaper journalist Sally Murrer in the UK under the Regulation of Investigatory Powers Act (RIPA); and HMRC identification of a whistleblower under RIPA.[18]

Furthermore, a three-year review published by the Interception of Communications Commissioner's Office (IOCCO) in 2015 showed that over 240 journalistic sources' communications data had been accessed between 2011 and 2014,[19] although there may have been other unrecorded incidents as well.

[15] http://www.nytimes.com/2010/03/31/world/asia/31china.html?_r=0. [16] https://cpj.org/2014/02/attacks-on-the-press-surveillance-storage.php. [17] http://ca.reuters.com/article/topNews/idCABRE94C0ZW20130513. [18] https://www.theguardian.com/politics/2014/mar/24/hmrc-criticised-mps-terror-law-tax-whistleblower-hodge. [19] http://www.iocco-uk.info/docs/IOCCO%20Communications%20Data%20Journalist%20Inquiry%20Report%204Feb15.pdf, p.29. The report states that 242 represents the maximum number of sources from 34 investigations reported by 19 police forces as there may be duplication.

Beyond that, a number of particular concerns about the law and legal environment were raised at the meeting.

- A first specific concern was that Lord Justice Leveson had recommended narrowing the protection afforded to journalists, against whom the authorities were seeking orders for disclosure of material, under PACE 1984. This recommendation, if adopted, would make it more difficult to protect sources, in particular because it could narrow the category of 'excluded material'.

- A second specific concern related to (what is at the time of writing) clause 34 of the Digital Economy Bill, which – if passed as currently drafted – will create a new offence for sources disclosing and journalists publishing information shared between government departments. Again, source protection would suffer if this clause passed.[20]

- A third specific concern related to the propensity of confidentiality clauses – for example, in employment contracts, dispute settlement contracts or procurement contracts – to deter sources from reporting their concerns. Particular mention was made of this in relation to the NHS, where the use and abuse of confidentiality clauses has attracted some scrutiny. There is protection for this in PIDA, but it has not been legally tested perhaps because it is difficult to find a claimant willing to spend the necessary time, energy and attention on the issue at the same time as risking their settlement award. Many whistleblowers understandably have other priorities, such as seeking employment, and getting on with their lives.

- A fourth specific concern was about the efficacy of whistleblowing protections. One participant argued that protections within PIDA 1998[21] needed strengthening. According to this specialist working with whistleblowers, PIDA has not been thoroughly reviewed by Government since it was enacted almost two decades ago and there is a real sense that this law is not working properly. There is a need for some strengthening provisions in the statute as well as some areas where the law could be simplified. Additional problems include access to employment tribunals becoming more difficult with cuts to legal aid, the introduction of fees and a creeping culture of costs. Given that these claims are often against employers with deep pockets more should be done by Government to protect whistleblowers who make public interest disclosures.

- A fifth specific concern related to the deficiencies of the Investigatory Powers Bill, being considered in Parliament at the time of the meeting and since passed by both houses in November 2016.

[20] https://www.publications.parliament.uk/pa/bills/cbill/2016-2017/0045/17045.pdf. [21] http://www.pcaw.co.uk/law-policy/a-guide-to-pida.

In particular, it was said that the Bill does not comply with the requirements of article 8 of the ECHR, as interpreted by the ECtHR, discussed above. As it was put to the group by one legal expert: 'Is there judicial oversight of a sort? Does the IP Bill satisfy article 10? No it doesn't'.

Such a view was supported by a human rights specialist, who said that the so-called protection in the Bill via an authorisation that has to be signed by a judicial commissioner is 'not protection at all'. Media representative groups including the News Media Association, the National Union of Journalists and the Media Lawyers Association have all made submissions to relevant Parliamentary committees on the Investigatory Powers Bill on this point.

Concern has also been raised about the definitions relating to journalism and journalistic activity which could be construed narrowly, and do not offer as much protection as the access requirements of PACE. And, as well as the clauses relating specifically to the protection of journalistic sources, areas of concern in the Bill included bulk personal datasets (BPD). It was suggested by one investigative journalist that 'risks will likely extend through the post hoc legitimation and extension of BPD'.

A participant from a human rights organisation also discussed the ramifications of the IP Bill on the way in which sources may view journalists and the inability of journalists to offer confidentiality. The sources may feel deterred and see journalists as proxy to the state due to their inability to protect sources.

While the IP Bill was of great concern to the group, views were divided on how much change could be made at a late stage of the Bill's progression through Parliament. The Investigatory Powers Act became law on 29 November 2016.

Definitional difficulties

While the discussion did not linger on definitions, or explore in depth the well-trodden ground of who constituted a 'journalist' or what qualified as a 'media organisation', these issues of definition were recognised by participants as being highly important. The issues here relate to who should be categorised as a journalist, as a source, as a whistleblower, and in general who merits protection and who does not.

Some examples of the difficulties that arise in practice from these definitional problems were raised. One example relates to David Miranda, the partner of the (then) Guardian journalist Glenn Greenwald who was stopped and detained by the Metropolitan Police at Heathrow Airport in August 2013 under the Terrorism Act 2000. By assisting his partner's journalistic activity, was David Miranda acting as a journalist or a whistleblower or a source? In *David Miranda v Secretary of State for the Home Department,*[22] the Court of Appeal found that 'stop' powers under Schedule 7 of the Terrorism Act 2000 were 'incompatible with article 10 of the Convention in relation to journalistic material in that it is not subject to adequate safeguards against its arbitrary exercise'.[23]

Another example that was raised was the case of a junior journalist at the BBC's panorama programme who disclosed confidential information about a journalistic investigation (amongst other things) [24] to the subject of that investigation, the politician Lutfur Rahman.[25] Was this act whistleblowing, which should be protected, a breach of confidence that should be punished, or a citizen-journalist acting as a source for a politician? If matters turn on one's political perspective, rather than on a general rule, enormous problems can arise.

One proposition to resolve the definitional difficulties was to argue that journalistic source protection should be afforded to institutional journalists, and made as robust as legal professional privilege (LPP).

LPP can be abused, and protection afforded for indefensible purposes, but such abuse of the privilege can be defended on the grounds that a rule is necessary to provide certainty and robustness. If such an argument works for lawyers, it was suggested, it could also work for journalists.

The deficiencies of this idea were discussed. An academic researcher was firmly of the view that it was inappropriate to offer protection of this sort only to institutional journalists. Part of the reason for such a view was that journalists frequently do not act responsibly. Also relevant, the researcher argued, was the risk of abuse by anonymous sources.

[22] [2016] EWCA Civ 6. [23] Ibid, para. 119. [24] The information was reported to have also included highly sensitive information about a terrorism investigation: http://www.independent.co.uk/news/uk/home-news/exclusive-bbcs-panorama-team-loses-confidential-information-relating-to-a-secret-british-army-unit-9580340.html. [25] http://www.bbc.co.uk/ariel/26834830.

The implication was that risk of abuse in the case of journalistic source protection was much higher than for lawyers. The researcher implicitly argued that, unlike Legal Professional Privilege, the merits of disclosure should turn on the particular facts in a given case. To support this viewpoint, they mentioned the Valerie Plame affair in the US in 2002-3.[26] Here, anonymous sources from the Bush administration were motivated to disclose certain classified information because of self-interested, partisan politics. The information that was provided was intended to discredit a retired diplomat, with whom the source in the Bush administration disagreed.

A response to this, later in the meeting, was that it might be appropriate to argue for stronger protection of journalistic sources and whistleblowers not by referring to journalists, or to the content in a particular case, but by emphasising the notion of the public interest in the existence of such a rule as a rationale.

One specific problem was raised concerning material derived from confidential sources that related to libel trials. In libel cases in the UK, for example, the general position is that unnamed sources can be relied upon when advancing a defence.

A difficulty here, though, was the potential weakening of any case for strong source protection rules for institutional journalists. This is because the focus is again on the type of information – being in the public interest – rather than the type of rule as being in the public interest. So the question of whether a source is legitimately protected returns to the nature of the information, rather than the relationship. This bears the risk of returning the resolution of the question once again to questions of political preference. However, the meeting seemed to be of the view that this was a more appropriate way of framing how journalist source protection should be conceived.

One specific problem was raised concerning material derived from confidential sources that related to libel trials. In libel cases in the UK, for example, the general position is that unnamed sources can be relied upon when advancing a defence. However, reliance on such sources can come at a cost, as they can be considered to have less evidential weight than attributed material. This is for a variety of reasons, such as the difficulties that arise in assessing the provenance of the information and the motives of the source when their identity is not known. In the US, in some states there is a starker choice – to rely on the source, the source will have to be identified. But where the judgment is that a source's identity should not be released, that will mean that it will be more difficult to defend a libel action, as their evidence may not be admissible in a trial.

[26] See, for example, Valerie Plame Wilson, *Secrets and Spies*, Index on Censorship, Autumn 2016: https://www.indexoncensorship.org/2016/09/does-anonymity-need-to-be-defended-autumn-magazine-2016/

Other legal concerns relating to ownership of information

Two other legal issues identified during the meeting involved the question of the ownership of particular journalistic information.

One related to notebooks and other journalistic records. 'Who owns these?', it was asked. Whereas notebooks are clearly the journalists' own, emails sent from work email accounts belong to the organisation, which means that the journalist has less control over access to their content. Ownership of the information (or practically speaking, possession of the manner or material in which the information has been recorded) is important it was argued. This is because in practice there are different consequences when information is sought from a journalistic organisation, or when it is sought from an individual journalist. If disclosure is sought from an organisation but an individual journalist owns (or practically speaking, holds or possesses) the material in question, then even if the organisation may eventually succumb to financial or legal pressures to hand it over, the journalist can still stand on principle and refuse to hand it over. Moreover, it was argued that the employer cannot – or may not wish to – force them to do so. In practice this may be useful to bear in mind, if disclosure is sought from a journalistic organisation, where that organisation wishes to withhold information.

A second, and different issue, involves the question of who owns the metadata relating to journalistic communication.

Neither the journalist, nor their employer, own this data. It is likely that it is owned by telecoms companies (or so one participant argued). This is important given the value of metadata in identifying sources (and, indeed, in identifying content). It amounts to an extra vulnerability that journalists face in attempting to protect their sources. They have no – or limited – control over the acquiescence with which telecoms providers respond to requests from governments for information that can disclose a source. This creates a weakness for those seeking to protect a source.

The Investigatory Powers Act appears to have adopted this view – i.e. the Government contends that because communications data obtained from a telecommunications provider belongs to the provider and not a journalist or journalistic organisation, issues to do with journalistic sources are somehow irrelevant.

Practical considerations

After the group had addressed the main legal concerns, the discussion turned to what happens in practice.

One issue arose from the account of the junior BBC Panorama journalist who disclosed information in the Lutfur Rahman case. This raised questions of access to information. There were practical questions that journalists and journalistic organisations need to address as to who should have access to what information, and under what conditions. An investigative journalist said it was inappropriate for interns to be given access to 'the crown jewels'.

Associated with this was the issue of investigators in non-traditional journalistic organisations – charities, and individuals. Such people might not have the appropriate structure and resources, or experience to investigate professionally, ethically, legally and safely. Moreover, they were thought much less likely to be able to deal robustly with bullying lawyers' letters, sent to silence them, than established news companies. And, apposite to the current discussion, they may well not have given thought to how – and to what extent – they should protect their sources. How, it was asked, 'can you spread a culture of protection?'

Somewhere between the two are freelancers, and non-traditional journalists such as bloggers. It is frequently unclear who, if anyone, bears professional responsibility for such people, when they are commissioned to undertake investigative work.

Questions raised by participants that related to source protection included: What does protection mean in practice? How far do journalists go with sources? Do you provide a source with a house if they lose their job?

Connected to the points discussed above in relation to the Valerie Plame affair, the motivations of whistleblowers and sources who seek anonymity were discussed. Some can be mischief-makers, and others may have an axe to grind. Responsible investigative journalists need to establish the motivations of their sources, and be alive to the fact that these may change. An investigative journalist described how early on in the conversation with a source, a journalist should act 'like a family doctor', and take a case history.

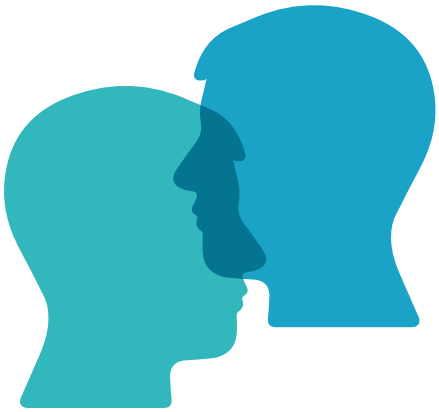
Conversely, many whistleblowers have taken great risks, and have undergone an exhausting process, to get to the stage of approaching a journalist. This needed to be taken into account, and indeed it was important for a journalist to be aware of the needs of a source, and to think hard about the extent to which such needs could be met – and their anonymity protected. Moreover, a journalist should ensure that a whistleblower understands what may result from their actions. Journalists should be aware of the psychological impact on sources, and not only focus on technical and legal risks. Specific training on source relations and support would be helpful here.

Questions raised by participants that related to source protection included: What does protection mean in practice? How far do journalists go with sources? Do you provide a source with a house if they lose their job?

It was suggested by a participant working with whistleblowers that news organisations should think about their rights and duties to whistleblowers. One area of potential action would be the introduction of a public interest defence for whistleblowers, which would extend beyond employment-related protections. This could help a whistleblower in their decision to share information. There was criticism of the extent to which the current regime of whistleblowing was effective. A measure of greater protection might improve the position of those who wish to report a problem in the public interest.

Importantly, it should be noted that an individual may not necessarily think of themselves as a 'source' when making contact with a journalist: they are simply sharing information about their observations or experiences.

Guarantees of complete protection of anonymity were highly unlikely to be achievable in a digital era, it was agreed. Everyone leaves digital footprints, everywhere. One journalist recognised that 'everything' they wrote down could be accessible in some way. The only safeguard was having face-to-face conversations.



An experienced investigative journalist described how perceived threats may in fact not be present, but the perception that they may be will have significant impact on what may be said or on what contact a source is ready to tolerate. Actual threats to sources may not be properly perceived. Information owners' knowledge of 'who knew what' may often be more important and effective than data potentially available from bulk data systems.

In other words, journalists should perform threat assessments while talking to sources, and also use these to ensure that they receive informed consent from the source, so that the source is clear that they know what they are getting into. There would be an important distinction as to whether the source is still employed in the workplace about which they are disclosing information. PIDA, which offers an employment-law related remedy to a whistleblower should they suffer workplace detriment, would be less useful in some circumstances – for example, if they are not seeking employment-related protection. One journalist made the point that there is a basic duty to protect communication with a source, even if the story falls through.

Others emphasised that, while a journalist should be straightforward and honest with a source about the risks, a balancing act was needed – as one journalist said, you do not want to 'spook the horses'.

There was an extensive discussion about the ethics of source protection. Where there was a legal compulsion to supply information to authorities, journalists would be presented with a moral choice as to whether or not to comply. To breach the confidentiality of a source would be in conflict with the National Union of Journalists (NUJ) and other industry codes. To an extent, this was a well-trodden discussion.

But the converse point was also raised. Some journalists may feel a moral obligation to provide information, even where there is no legal compulsion. This may occur when, for example, an investigation uncovers serious criminality. The journalist then has to make a judgement about whether to give evidence in a case. An investigative journalist said such dilemmas arise practically daily.

Morally, it may seem clear that they should. But this leads to difficulties down the line. First, when a journalist begins cooperation, it becomes difficult to retreat at a later stage. A journalist – and an organisation – becomes boxed in.

The journalist then has to make a judgement about whether to give evidence in a case. An investigative journalist said such dilemmas arise practically daily.

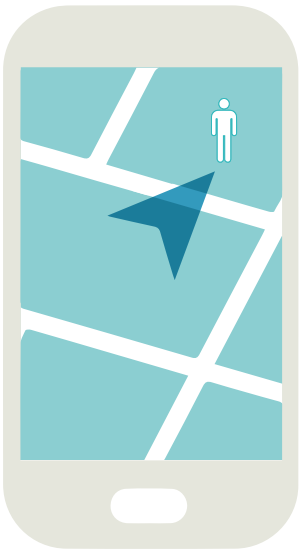
Secondly, cooperation with authorities on a first occasion may create a precedent, which could make it more difficult for a journalistic organisation to resist a request from the police to comply on a later occasion. It is easier for an organisation to say 'we do not supply material unless you get a court order compelling us to do so'. In practice, in other words, a journalist who hands material over or works with the authorities because they feel a moral obligation to do so, may create difficulties on other occasions, or where others do not feel so obliged.

Particular practical concerns aligned to this arose in relation to terrorism investigations. One investigative journalist described how the duty to inform the authorities about certain information under s19 of the Terrorism Act 2000 results in a chill on investigative activity. He said that he has refrained from investigating material, because it could result in his having to inform the police, which could compromise his sources.

One personal vulnerability for journalists related to terrorism, occurred when police categorised journalists as domestic extremists. This has been revealed through work by the National Union of Journalists, and individual subject access requests under the Data Protection Act. If journalists are categorised as such, they are likely to find their activity is monitored.[27]

[27] https://www.nuj.org.uk/news/journalists-catt-challenge-extremism/.

Technological factors



Throughout the discussion the group considered technological issues.

At a very basic level, questions were raised about the safety of secure online drop-box type systems that have been introduced by some organisations. Digital footprints were inevitable. Furthermore, one might not be aware of the full digital trail if intermediaries were involved. Jigsaw identification via several pieces of information was a possibility.

Anonymous secure drop-box systems posed their own problems, it was said. They make it impossible, or very difficult, to assess the motivations and provenance of material derived from them. That means it is difficult for a responsible investigative journalist to use the material delivered by them.

Related to this point was an issue of continuing and maintaining contact with a source, not just securing the first point of contact. OnionShare was mentioned as one potentially useful tool.

Risk assessment was identified as essential, and this required thinking beyond one investigation – if a journalist has material relating to different activity stored on a machine this is also vulnerable to hacking.

Concerns were raised about cryptography techniques, including the use of the encryption programme Pretty Good Privacy (PGP), and the difficulties of doing it correctly. PGP was essential to Glenn Greenwald's reporting of the Snowden revelations, but the appropriateness of information security methods will depend on a case by case analysis. There is a very important place for PGP but, as with all methods, it is not a silver bullet remedy.

At several points, it was suggested that old fashioned and pre-digital methods could still serve a purpose: e.g. receiving information by post, fax or hand-delivery.

It was suggested that journalists could advertise online when they will be in the office, so an individual could find them in person (this would not necessarily help a freelance without an office base, and such source-journalist contact could still be vulnerable to surveillance – by tracking smart phone locations, for example).

The participant working with whistleblowers suggested that many people do not think about encryption. For a source, the main concern is going public, and if dealing with the media, to what extent they trust the journalist.

One opening presentation suggested: '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'.[28]

[28] Smyth and O'Brien, *CPJ Journalist Security Guide: Covering the News in a Dangerous and Changing World* (New York: Committee to Protect Journalists, 2012), 17.

10 recommendations

The discussion was wide ranging, with participants disagreeing on some of the elements summarised above. However, the following suggestions for different stakeholder groups were suggested for future initiatives.

For Policy Action

We recommend that policymakers and lawmakers:

1 Guarantee that the Investigatory Powers Act Codes of Practice protect journalists and their anonymous sources. Now the Investigatory Powers Act is passed, ensure that the associated Codes of Practice sufficiently protect journalists and their anonymous sources, in ways compliant with the UK's international human rights obligations.

2 Make certain that the judicial oversight regimes are designed and operate in a way that sufficiently protects journalists and their anonymous sources. A key element of the oversight regime will be the publication of regular reports on the usage of intercept requests. Policymakers should recognise that it is appropriate for media organisations to push for as much detail as possible in order to assess whether warrants are being misused.

3 Ensure that Part V of the Digital Economy Bill is amended, so that it does not criminalise appropriate disclosures by whistleblowers operating in the public interest. The regime in Part V (clause 34) of the Digital Economy Bill would have the effect of criminalising any onward unauthorised disclosure of the information. The Media Lawyers Association suggest that this 'creates new and anti-democratic restrictions on how that data can be treated by journalists, which would appear to seriously threaten (and gag) legitimate journalism'. Based on this analysis and the discussion at the meeting, it is recommended that this clause is re-drafted to ensure compatibility with article 10 of the ECHR, as required by law.

For Journalists and News Organisations

We recommend that journalists and news organisations:

4 Strengthen policies on secure technology, source care and protection. The Centre of Investigative Journalism has produced a useful resource in the form of an Information Security handbook.[29] Organisations that support the work of journalists, including the National Union of Journalists, can also provide journalists with training and resources. Old fashioned and pre-digital methods could still serve a purpose, although these are not necessarily fail-safe: e.g. meeting in person, receiving information by post, fax or hand-delivery. They should also consider the position of self-employed freelancers who may be vulnerable to legal and technological threats.

5 Review how they engage with sources that wish to remain anonymous. This may be based on existing work in this area, including the Neil Report produced by the BBC.

6 Undertake sufficient training on source protection. Journalists working with confidential sources should be given more training on the practicalities and limitations of source care and protection. Training should cover a range of factors: legal, technological and psychological, and should not only consider methods by which sources can be protected, but also the limitations of that protection. This should be communicated to any source to whom confidentiality is promised. This type of training should also be offered to trainee journalists. Universities and other organisations offering journalism training should make such training an integral part of their courses.

For Researchers and NGOs

We recommend that researchers and NGOs:

7 Examine the merits of extending public interest defences for whistleblowers. This research should consider public interest defences that extend beyond employment protection remedies, and into the law of confidence, for example.

8 Analyse and see what can be learnt from whistleblowing legislation in other territories. Australia and Ireland provide examples of countries with specific legislation on whistleblowing. Mandatory procedures for whistleblowing could help facilitate and legitimise people in speaking up.

9 Seek adequate definitions of journalism and journalists. These remain uncertain in law. In-depth analysis and research, both doctrinal and empirical, would inform the drafting of future legislation that offers specific protections for journalistic source material. Key questions include:

- Whether these protections that focus on protecting public interest activity should go beyond journalists to investigative not-for-profit organisations and others.
- The viability of the argument that there should be a rule-based protection for journalistic source protection, analogous to that which exists for lawyers. This might be explained with reference to the public interest in such a rule existing.
- Whether it is better to adopt as a default position a case-by-case, ad hoc analysis, as to whether a source should be protected on the basis of whether the disclosure of that information was in the public interest.
- Whether there are viable and useful definitions of 'news', 'journalism' and 'journalists' that can be found in other areas of law or in other jurisdictions – for example, in copyright and defamation.

10 Produce a public log of cases where source protection is breached, and in what ways. The discussion revealed a range of different experiences and responses to pressure from state authorities and agencies for source disclosure. Empirical research would assist in the following areas:

- What is actually happening? Work should be done to survey and interview the different actors involved in the process of whistleblowing, to gather data on the implications of different rules and approaches in practice.
- How can it be categorised? Work should be done to evaluate and classify the nature and type of material published and gathered as a result of anonymous sources, to assess the extent to which this material could be seen as 'public interest' material, however that might be defined.

Future plans

The authors of this report propose to:

- Set up a mailing list to develop a rapid response group of informed people to respond to policy developments (such as new laws) affecting investigative journalism and source protection.
- Explore the possibility of future research and research impact funding. This would build on the findings of this meeting and other relevant projects.
- Undertake further empirical research and provide periodic updates on the severity of the threat to source protection in 2017.
- Encourage the formation of an all-party group in Parliament which would have the capacity to highlight and examine issues of source protection and related threats to public interest journalism. The House of Lords Committee on Communications report on the future of investigative journalism in 2012, provided a welcome – albeit fleeting – moment of focus on the challenges facing journalists and the media organisations they work for. Many of the recommendations contained in the report have yet to be pursued. The establishment of an all-party group could act as a continuing forum for dialogue about the importance of investigative journalism, the need for strong source protection, and the challenges posed by government legislation.
- Add further resources to a project website page. This report would be published on this page, along with other materials.

Judith Townend

Lecturer in Media and Information Law, University of Sussex and Associate Research Fellow, Information Law and Policy Centre, Institute of Advanced Legal Studies.

Contact: judith.townend@sussex.ac.uk

Richard Danbury

Principal Lecturer, Channel 4 Investigative Journalism MA, De Montfort University Leicester, and Associate Research Fellow, Information Law and Policy Centre, Institute of Advanced Legal Studies.

Contact: richard.danbury@dmu.ac.uk[i][ii]

[i] With thanks to all the participants for sharing their wide and in-depth knowledge of this area, especially those who prepared opening presentations for the discussion. Acknowledgement is also due to Jenna Corderoy for her assistance in note-taking and Dr Daniel Bennett for research support. [ii] All hyperlinks in footnotes correct and accessible at the time of writing.

Information Law and Policy Centre, Institute of Advanced Legal Studies: An initiative supported by Guardian News and Media

IALS INSTITUTE OF ADVANCED LEGAL STUDIES | SCHOOL OF ADVANCED STUDY UNIVERSITY OF LONDON