Chilling effect: regional journalists' source protection and information security practice in the wake of the Snowden and RIPA revelations

Paul Bradshaw
School of Media, Birmingham City University, Birmingham, UK
01213315367
Paul.Bradshaw@bcu.ac.uk

Abstract

Despite reports of widespread interception of communications by the UK government, and revelations that police were using surveillance powers to access journalists' communications data to identify sources, regional newspaper journalists show few signs of adapting source protection and information security practices to reflect new legal and technological threats, and there is widespread ignorance of what their employers are doing to protect networked systems of production. This paper argues that the 'reactive' approach to source protection, that seeks to build a legal defence if required, is no longer adequate in the context of workforce monitoring, and that publishers need to update their policies and practice to address ongoing change in the environment for journalists and sources.

Keywords

Security, journalism, sources, privacy, encryption, law, surveillance, anonymity

Introduction

In early 2014 the UK's Metropolitan Police was closing Operation Alice, its investigation into an altercation between a senior politician and a police officer which was leaked to a national tabloid newspaper ('Plebgate'). In its closing report it was revealed that the force had used surveillance powers granted under the Regulation of Investigatory Powers Act (RIPA) to obtain the phone records of reporters and editors at *The Sun* newspaper without notification or any opportunity for legal defence.

Coming less than 12 months after Edward Snowden's revelations of widespread interception of communications by the US government and its 'Five Eyes' partners (the UK, Australia, Canada and New Zealand), this brought information security and source protection issues even closer to home for newspaper reporters who might have thought themselves unaffected. Eventually, as other police forces' use of the same powers were revealed, this would include regional newspaper reporters too.

As this research finds, however, regional newspapers have not adapted their practices to respond to new legal and technological developments, and journalists have little awareness of what employers are doing to protect production systems. It argues that the reactive approach to source protection, based on constructing a possible legal defence, is inadequate, and that instead publishers need to more proactively design threat models and sourcing policies which address the tracking of sources' 'data trails' by both the state and employers.

The field of journalism studies contains very little literature on the security services (Bakir 2015) and even less on security and surveillance (Spaulding 2009). While there has been a range of recent research into the Snowden revelations (Mols 2015; Haim 2015; Backman et al 2015; Ahmad & Hussain 2015), the practices of US investigative journalists (Pew Research Center 2015), and, more broadly, emerging threats to freedom of speech and source protection internationally (two of the three 'emerging threats' identified in Freedom House's Freedom on the Net 2014 report relate to information security), no research has yet been undertaken into the more everyday practice of reporters and editors on regional newspaper titles in the UK.

Recent research on protection of sources claims there is a need for increased awareness (Kleberg 2015) based on anecdotal evidence, but there is no quantitative basis for those. Similarly, claims by Guardian editor Alan Rusbridger that most news outlets "don't even begin to deal with [the issue on online security]" (Journalism.co.uk, 28 March 2014) bear further scrutiny.

The changing nature of source protection is particularly highlighted by details in the Operation Alice report which include analysis of one political editor's mobile telephone records and records of incoming calls to the news desk. Notably, the connection between reporter and source was made indirectly:

> This application produced five telephone numbers, all of which were researched for connections with the MPS [Metropolitan Police Service]. One number was identified as the switchboard number for Hinchingbrooke Hospital in Cambridgeshire. It was established that Officer 15 DPG's wife Member of Public 3, was employed at that hospital
> Enquiries were made with Siemens in order to identify from the data on the exhibit, which extension within the hospital the call to The Sun was made from. (Metropolitan Police 2014, 34)

Suffolk Police had used RIPA in 2006 to identify the source of a story about the re-opening of a rape investigation, and Thames Valley Police's decision to to bug a journalist's car in the same year was revealed to have been granted under the same law. Kent Police had used similar powers to access one reporter's landline and mobile phone records. And on 29 October 2014 Press Gazette reported that Derby City Council had used RIPA to spy on an employee's meeting with a local journalist who was investigating allegations of wrongdoing within the council's environmental services department. Unusually, this was undertaken in an overt manner so that both employee and journalist were aware of the surveillance. The employee later ended communications with the journalist.

The repeated revelations led to a critical report from the Interception of Communications Commissioner's Office (IOCCP) which identified 19 police forces accessing journalists' communications data in the 3 year period covered by the inquiry, 105 journalists and 242 sources including staff in the police, prison, hospital and military services, and those in central and local government. An amendment was subsequently made to section 71 of RIPA 2000 as part of the Serious Crime Act in March 2015. This required the revised code "to include provision to protect the public interest in the confidentiality of journalistic sources" (Interception of Communication Commissioner's Office 2015c).

Despite this, in the few months following the amendment to RIPA two police forces were found to have acquired communications data related to journalists without obtaining judicial approval. The IOCCO also expressed concerns over the vague wording of the amendments which allowed forces to acquire journalists' communications data *without* judicial approval in order to corroborate sources who were already known to the police. And, as this research shall explore, wider legal and technical trends suggest journalists should not assume that prior notification will be the first step to source protection.

Source relations

Source relations are inherent in two of the four democracy-related roles of news identified by McNair - those of mediator and/or representative of communities and an advocate of the public in campaigning terms - and typically form a key role in a third: the watchdog/fourth estate role (McNair 2009, 237-240). Notably, regional journalists themselves describe their role in similar terms around the watchdog role, autonomy from the council and acting in the public interest, all of which rely in part on having 'inside' or 'unofficial' sources (Firmstone and Coleman 2014).

Despite this, literature on journalists' relations with sources tends to focus on routine sourcing practice and reliance on public relations (Franklin 2011; McNair 1998) with respect to the impact on gatekeeping and news values, rather than non-routine sources and source relationships.

Journalists' need to protect sources represents one of the most central ethical considerations of the profession (Brand 2006). The "chilling effect" that disclosure can have (Goodwin v United Kingdom 1996) includes an increasing unwillingness to give journalists valuable information, so

that the public is left uninformed on key issues (Penrod 2004), as well as reluctance by journalists themselves to investigate issues: in 2015 14% of US investigative journalists said that concerns over surveillance had prevented them from pursuing a story or reaching out to a particular source, and 2% had considered leaving the profession entirely (Pew Research Center 2015).

Research outside of the Western sphere suggests that journalists change their own information flows in the context of awareness of surveillance practices (Cheng and Lee 2015). But while formal access to internal sources is narrowing due to increasing control by media relations professionals (O'Neill and O'Connor 2008) new technologies are both broadening and limiting journalists' access to new sources (Matthews 2013; Van Leuven et al 2014; Williams, Harte and Turner 2015).

Kevin Marsh, for example, notes of investigative journalism that: "Leaking and whistleblowing have moved from a largely individual occupation onto an industrial scale, bringing huge amounts of what was previously secret into the open." (Marsh 2013, 233)

Wikileaks, Cryptome, and dozens of similar platforms have provided organisational and technical support for such leaking practices (Greenberg 2012), while the 'hacktivism' behind the Ashley Madison and Hacking Team leaks has added a cultural dimension, and Russia and China's suspected involvement in the Sony and Democratic National Committee leaks has added a political dimension.

This may only be a temporary shift, however, as monitoring of leaks and whistleblowing could be argued to have similarly moved onto an 'industrial scale' footing, as it becomes "ubiquitous … in both the political (public) and civil (private) sphere of society ... endemic to large scale organisations." (Zureik 2003, 42) This is particularly exemplified in software used by corporations to identify or prevent leaks, including "data loss prevention" (DLP) software which looks for sensitive information in outgoing data traffic; "network forensics" which looks for suspicious patterns and "bells in the dark" designed to identify people accessing information they shouldn't (Economist 2011).

Legal context

While privileges protecting anonymity in communication with lawyers, priests and doctors seek to "encourage candour so that the listener can better aid the speaker" in a number of countries this is not necessarily the case in journalism (Bates 2010, 10-13). And these privileges have become uncertain in the context of mass information gathering practices.

A number of laws in the UK require communications providers to provide 'real-time interception' of communications and disclosure of customer data. Vodafone's Law Enforcement Disclosure Report identifies these laws in 29 territories in which it operates. Of the UK it notes that s.5 of the Intelligence Services Act 1994 (ISA), provides authority for MI6 and GCHQ to conduct intelligence activities in the interests of national security, the prevention or detection of serious crime, or in the interests of the economic wellbeing of the UK, without the service provider necessarily being aware (Vodafone 2015).

Under Section 8(4) of RIPA grounds for suspicion are not required to obtain an 'external warrant' certificate to intercept and store 'external' communications, including those using web services based outside the UK even when used by UK citizens (Farr 2014). Outside of RIPA, this framework is also reported to be the basis for GCHQ's Tempora programme which, according to a 21 June 2013 Guardian report, stores data drawn from fibre-optic cables for up to 30 days so that it can be sifted and analysed.

Most of these laws are broad enough to target protest groups (Anderson 2014), while examples of such broad classification in the UK include anti-capitalist movement Occupy London being listed by police in a counter-terrorism presentation alongside Al-Qaida, and surveillance being employed against campaigners targeting corporations (Lubbers 2012) and environmental activists (Evans and Lewis 2013).

The powers could also potentially be used against UK journalists reporting on uprisings in other countries. An earlier review on the operation of the Terrorism Act 2000 and Part 1 of the Terrorism Act 2006 raised concerns that definitions would take in actions which were intended to take place outside the UK, and which "might otherwise constitute lawful hostilities under international humanitarian law" (Anderson 2012, 33). The same review also raised concerns about the requirement in section 38B to inform the police about terrorism and the impact of that on a journalist's duty to protect sources (Anderson 2012).

In July 2013 the UK rushed through emergency legislation - the Data Retention and Investigatory Powers Act (DRIPA, sometimes DRIP) - which amended the RIPA act and extended interception capability to cover non-UK providers and conduct outside the UK. An open letter by UK legal academics described it as introducing "powers that are not only completely novel in the United Kingdom, they are some of the first of their kind globally." (Marsden 2014)

A code published following a consultation on communications data codes of practice confirmed that journalists would not be protected (Home Office 2015). In July 2015, however, the high court ruled that the Data Retention and Investigatory Powers Act was "inconsistent with European Union law" largely due to two weaknesses: the lack of a definition of "serious offences" and provision for independent scrutiny to ensure that surveillance is "strictly necessary" (EWHC 2015). An appeal against the ruling was referred to the European court of justice.

Much of the defence of data-gathering practice revolves around the distinction between 'content' data (what was actually said by the source or journalist) and 'meta' or 'traffic' data (who was communicating with whom, when and where). Leistert (2008) argues that the distinction is misleading:

> The person calling the crisis line is not ordering pizza. There are undeniably *semantic elements* in the mass of so-called traffic data … The caller's ID is a device ID. The profiler's assumption that the device is equal to, or identical with, or identifiable with its user is an obvious *pragmatic* reduction ... retaining traffic data *shifts* the *address space of meanings* from machinic to human … it is transformed into the symbolic: it now *represents* the movements and telecommunication acts of people (Leistert 2008, 927-8)

Outside of legal means, journalists can also be targeted by spammers who wish to hack their accounts, or organisations who wish to supply misleading information to journalists using practices such as astroturfing (campaigns which purport to be 'grassroots' but are actually sponsored by powerful interests) and sockpuppetry (the use of fake online profiles to propagate opinions). Bakir (2015) for example notes that GCHQ's Joint Threat Intelligence Group (JTRIG):

> Possesses among the following tools for online covert action: 'CLEAN SWEEP' that can "Masquerade Facebook Wall Posts for individuals or entire countries," 'GATEWAY' that can "artificially increase traffic to a Web site," and 'SLIPSTREAM' that can "inflate page views on Web sites" … 'CHANGELING' [provides] "the ability to spoof any e-mail address and send e-mail under that identity" and 'HAVOK,' a "real-time Web site cloning technique allowing on-the-fly alterations." (Bakir 2015, 133)

Tools and techniques are not limited to state actors. When the Associated Press's Twitter account was hacked by the Syrian Electronic Army it was attributed (in a Quartz article on April 23, 2013) to a 'phishing' email. Similar techniques were blamed for a data leak at the New York Times reported by the newspaper on January 30, 2013, while "spear phishing" intended to obtain login credentials, has been employed against the New York Times, Global Post, CNN and Forbes (Freedom House 2014, 10). Often it is the audiences that hackers are interested in: in 2009 a malicious link was inserted in an email sent by Reporters Without Borders to its supporters, infecting the computers of those who clicked on it, and the New York Times "inadvertently served

malware to some of its visitors" (Morozov 2011, 147). Research in 2015 found that more than 58 percent of online advertisements with hidden malware were delivered through news websites and entertainment websites (Bromium Labs 2015).

Crime and national security reporters are not the only ones affected. On May 4 2013 the New York Daily News reported that entertainment website E online had had its social media account hacked while on July 27 2015 Quartz reported that New York Magazine was reportedly hacked over a story about women claiming to have been raped by Bill Cosby. On the same day Elle reported that anti-abortion activists had hacked the emails of Planned Parenthood.

These changes take place in a wider legal context of unclear privacy laws (Dawes 2013), while concerns about surveillance of journalists relate not just to present governance but to future systems as well, given the permanence of digital history (Brake 2014), the increasing role of private corporations, and historical uses of surveillance powers not only against journalistic sources but journalists themselves (Theoharris, 1985). The 1974 Privacy Act, for example, was passed in the US after Richard Nixon used the Internal Revenue Service to audit the tax returns of individuals including journalists. But private data repositories now offer a loophole (Abelson, Ledeen and Lewis 2008).

Methodology

Based on the discussion in the previous section, this research seeks to answer the following research questions:

RQ1: What level of awareness exists among regional journalists of information security (infosec) issues?

RQ2: How does that awareness translate into action, and workflow?

RQ3: How does the typical workflow of regional journalists translate into a threat model which might be used within the industry?

The study used face-to-face surveys of 76 regional journalists at a number of publications within five newspaper groups in the UK, 10 in-depth interviews, and analysis of policy documents. The research was conducted over 5 field visits in June and July 2015 to regions across the UK. Participants were selected based solely on their presence in the newsroom in order to get the widest cross-section of respondents.

[INSERT TABLE 1]

It is important to understand the assumptions made about the research context but it is also important to understand the role of the researcher and to understand how his prior values and knowledge will influence the research process. This includes cultural background, intellectual position, gender and political values as well as many others (Easterby-Smith et al 1998; Bryman 2001). I employed reflexive practice based on my own experience as a journalist working with a range of news organisations.

Researching journalists' use of security practices has the potential to expose practitioners to surveillance themselves, much as researching activism presents the same risks (Flacks 2005). Although journalism might not be considered a 'social movement', it does often involve reporting on such movements (Evans and Lewis 2013), and so the researcher was conscious of the ethical obligation to provide "knowledge that is both useful to and respectful of social actors" (Milan, in Della Porta 2014, 450).

Milan (in Della Porta 2014) argues that researchers should encourage activists to use email encryption and routing software. However, when the subject of the research is itself the use of such

technologies, such processes would represent an interference with the subject resulting in an inaccurate representation of the field. It would also restrict research to those subjects willing to learn such technologies, leading to a highly unrepresentative sample.

Instead, then, it was important that a methodology was established which minimised the risk to participants. This was done in a number of ways. The first step was the establishing of a 'threat model' (Carlo and Kamphuis 2014) to assess which information collected and generated during the research may need to be protected, and means by which risk might be reduced.

The survey stage was conducted on paper and in person on location at a number of newsrooms in order to ensure that individual responses could not be connected with individual journalists. Demographic data was not collected and names were not used either in the collection or the presentation of results. Once collated into aggregate form, original paper responses were destroyed.

This meant that a smaller sample was collected than would have been the case had the survey been distributed electronically or via post. However, this did address some weaknesses of survey approaches (Bertrand and Hughes 2005): namely that respondents would be self-selecting and the results not generalisable.

Conducting the surveys in person allowed for conversations that confirmed this: many respondents did not feel the subject of information security applied to them, and therefore would likely not have responded to a survey distributed in other ways. This highlighted a significant issue in information security within newsrooms: that it is perceived to only be required for journalists rather than sub editors or other editor roles, and only for journalists who have contact with particular types of sources, for instance those in the field of crime. In one major regional newsroom not one journalist was motivated enough by the topic of source protection to put themselves forward.

[INSERT TABLE 2]

Survey design replicated the Pew study of investigative journalists (Pew Research Center 2015) in order to allow for comparability, while an analytical interview approach was adopted as journalists are familiar with the interview situation and the process involved, and the interviewee had a particularly deep knowledge of the subject matter involved (Malmelin and Villi 2015; Kreiner and Mouritsen 2005).

Interviews lasted for an average of 60 minutes and were semi-structured. Topics covered included journalists' workflows when dealing with sources and documents, organisational and individual approaches to information security, and understanding of the Snowden and RIPA revelations.

Interviews were organised verbally and a protocol established to minimise the risk of eavesdropping, including the switching off of mobile phones and other electronic devices and the placing of phones in a Faraday cage (Carlo and Kamphuis 2014). Recordings were made using a device which was not - and would not be - connected to the internet. Notes were then taken manually so as not to create a digital record. Although such procedures were largely rendered unnecessary by the contents of interviews, it was not possible to anticipate this.

Results

In contrast to the Pew study of investigative journalists, no regional newspaper journalist surveyed in the research said that concerns over surveillance had led them to consider not covering a story or reaching out to a source, and there was a broad consensus that security issues did not affect them or their work. Respondents repeatedly noted that they had not altered their practices.

Despite this, survey results showed a majority of journalists had changed *some* behaviour relating to infosec (documents, internet research or communicating with sources or other

journalists) in the last 12 months. And there was some awareness of the dangers of particular methods, such as sending a document electronically due to metadata associated with it.

The areas which saw the highest proportion of journalists change their behaviour was the use of the internet for researching stories (just over half had changed their behaviour) followed closely by source communication and the sharing or storage of documents (48%). 42% had changed their behaviour when it came to communicating with other reporters and editors, and just under a third of those asked felt that they had changed the way they assessed risks.

[INSERT TABLE 3]

A significant minority of journalists had very poor information security practice: more than one in five journalists did not use different passwords for different online accounts. And 16% of journalists did not do *any* of the following: use different passwords, clear their browser history, turn off cookies, turn off geolocation or use enhanced privacy settings on social media.

[INSERT TABLE 4]

There was widespread ignorance of information security policies and technologies put in place by the publisher: the vast majority of respondents did not know if their employer had taken any steps to protect journalists (88%), while a further 6% thought that they had not done so. Only 3% thought their employer had taken steps.

[INSERT TABLE 5]

Despite this lack of awareness about any new steps, 31% of journalists still felt confident enough to say that their employer was "doing enough" to protect journalists. This seemed to be based on their own experience - "Well they must be doing something. I haven't been hacked" - or by implicit trust in other parts of the organisation: "I can only assume that our security is very good," explained one source. "You assume [measures from the more important publications] filters down to you." (Respondent C 2015)

[INSERT TABLE 6]

47% of journalists did nothing to protect their sources in terms of meeting in person, avoiding third party email servers, using fake email accounts or usernames, turning off phones, or using encryption. 12% of respondents felt that none of the source protection techniques applied to them and a further 9% felt that at least one of the techniques did not apply to them.

The most common technique used to protect sources - mentioned by a third of respondents - was to meet in person. Notably one in five respondents had started to meet sources in person in the last year. One in ten respondents avoided third party email services such as Gmail and Hotmail. 5% turned off electronic devices when meeting, and 4% used fake accounts. Only one journalist used email or messaging encryption: the tool WhatsApp, also the only tool used to protect information or sources that any respondent was able to mention (1 respondent).

[INSERT TABLE 7]

In interviews journalists avoided responsibility for their information security behaviour in three key ways:

1. Firstly, respondents identified security concerns as something which did not affect them directly, either because they did not do the type of journalism, or cover the sort of subject,

which they felt that it did affect. Reinforcing this was a lack of awareness of how laws such as RIPA operated, and a perception that it related specifically to the police (some journalists had also not heard of the Act).
2. Secondly, infosec practices were delegated to sources, who were treated as relatively security-literate and not in need of assistance.
3. Thirdly, there was a fatalistic resignation to the fact that certain organisations would be able to access their communications regardless of anything that they did.

"Another planet"

Both in surveys and in interviews, protection of sources and of communication was described as something which was only of concern to particular types of journalist. "We're a community newspaper and this [information security] seems like another planet," noted one respondent (Respondent B). "The regional press don't feel that a lot of what we do would be on the radar of [public bodies] and therefore it's not something we'd particularly [focus on]" (Respondent C).

But senior editors trust those reporters dealing with sensitive information to understand how to protect sources: "The type of reporter who would be dealing with an issue like that," said one respondent, "is someone who is usually pretty conversant with that kind of issue. So they might operate in a certain way." (Respondent C)

However, when those most likely to be affected by security issues - crime reporters and those involved in investigations - were asked about their information security processes, it was clear that source protection behaviour had not changed to address RIPA or recently emerging technical vulnerabilities. This was reflected in a lack of internal guidance.

It was clear from descriptions of the workflow involved in sensitive stories that editors may also need to be careful about their communications: reporters, for example, would typically correspond with their editor about sensitive sources and considerations regarding health and safety or legal action.

"People are pretty savvy"

While journalists and editors did not feel that *they* had changed their behaviour regarding information security, they believed that sources were already aware of the need to be careful about communications:

> In most cases people are pretty savvy in terms of protecting themselves because if someone's coming to us I wouldn't necessarily say to them don't use your work email because usually if they're whistleblowing types they won't be using their work email and if they wanted you to phone them you would phone them at a set time where they were in an environment where they can use their private mobile (Respondent C)

Substantive detail was avoided in emails, and phonecalls were used to arrange a meeting or an outside-working-hours call. "But that's not systematic and encoded in any way." (Respondent A). And when reporters received documents it was often from an email account "which has clearly been set up purely to send that document." (Respondent B).

Where journalists had changed their behaviour it was attributed more to 'putting the source at ease' than genuine information security, and it may be that social capital is more relevant in this respect than strictly utilitarian considerations (Lewicki and Brinsfield 2009).

"They can get access to anything they want to"

There was also a resignation to widespread data gathering and interception:

> We're probably all being watched but I just feel that what I do... There's a kind of trust I suppose, in the powers that be and also that you're operating at a certain level that they wouldn't be interested in. They're so sophisticated that the little things we do to protect sources might protect a council employee but if they wanted to find out who it was they wouldn't have a major problem with it. (Respondent C)

Finally, interviews with senior reporters suggest an ignorance of the way that laws such as RIPA allow public bodies to access journalists' communications without the journalist having an opportunity to argue against that (or any awareness that this is happening).

One experienced crime reporter, for example, said that "As a rule of thumb [Snowden and RIPA] has sharpened our reflection on whether a story is in the public interest" (Respondent D), suggesting that such an argument would be part of a defence against attempts to force the journalist to reveal their source.

> I've had the force simply verbally asking where have you got this information from because it was very close, and it's gone no further than that, and in fairness they've never taken action to gain that information from me.
> Our fundamental concerns haven't changed: is this person reliable, and if things do go pear-shaped where do we stand on this? (Respondent D)

But if RIPA or other means had been used, the journalist would *not know* - unless they had used the Data Protection Act or Freedom of Information Act to request details on such activities.

Analysis

Historically, protecting sources has been a *reactive* process: one that only begins *after* the contact has been made. Respondents' statements about checking the validity of sources' claims and discussing those with editors reflect a 20th century world where sources only needed protecting once information was published and the journalist's main defence was legal. Similarly, 'normal' regional newspaper journalists' belief that information security issues did not affect them because they are not directly dealing with sensitive sources reflect a world where their colleagues would always be targeted directly.

This is reflected in the literature too: Carlson argues for "careful consideration of unnamed sources weighing their potential benefits with their actual use" (Franklin and Carlson 2011, 43), but this careful consideration cannot be made *before* the fact.

The contemporary context for journalists and sources presents a very different problem in four specific aspects:

1. Identification *before* publication through algorithmic and routine monitoring of communications not only by intelligence services but also employers.
2. *Retrospective* identification through similar means
3. The shift from a legal defence to a legal *and technical defence*
4. *Indirect targeting* of journalists through colleagues and systems

An example of *retrospective* identifcation comes in Operation Alice where, once sources were identified, further analysis was conducted on individuals' web searches (including search terms

relating to newspaper staff), WhatsApp messages (including images) and browsing history (including newspaper articles) (Metropolitan Police 2014, 34).

In this context, increasingly, protecting sources may have to become more proactive. One initiative being taken by news organisations, as reported by Nieman Lab on July 13, 2015 for example, is to switch from http to the more secure https protocol.

On the shift to a legal *and technical defence* in most known cases involving communications interception the journalist has *not* been provided with an opportunity to argue against access to communications data. Although this aspect of RIPA was changed with the Serious Crime Act in 2015, on July 22 2015 Press Gazette reported that there had already been a subsequent application where a judge was involved but the journalist was not put on notice.

It is not just legal avenues where the organisation may not be aware of attempts being made to access sources or systems. The remote access of journalists' computers at Al Jazeera and surveillance of Der Spiegel were only revealed years after the acts had taken place, while a UNESCO report notes that "News organizations and individual journalists do not often know or share that they have been victims of digital attacks." (Henruchsen, Betz and Lisosky 2015)

On targeting *indirectly* there is evidence of both widespread ignorance of the legal means available to authorities, and technical vulnerabilities. While one respondent based their perception of organisational security on the belief that they had not been hacked, another admitted "There was one person who had their account hacked by spammers 4 times in about 6 months." And broadly respondents were unaware that accounts might be hacked without users being aware of the fact. In IT policies employees are told to contact the IT department only if the computer "behaves strangely or you suspect it may have a virus" (Policy Document 1).

Internal policy guidance at regional news organisations lacks specific guidance on information security. The policies suggest that the journalist "change your passwords regularly" (Policy Document 1) but does not outline practices for choosing good passwords, or a desirable frequency. Although system passwords are force-changed every three months, in at least one organisation there are no such procedures in place for external system passwords such as social media accounts.

No guidance is given about the risks of using public wifi (Kleberg 2015; Price 2016), although there is increased use of VPNs to protect core systems such as the content management and email systems.

In interviews and conversation reference was often made to the use of mobile phones in following up initial contacts as a way of protecting sources. But in using RIPA powers, as noted in a July 21 2015 Press Gazette article, at least one police press office assisted officers in providing the mobile telephone numbers of journalists, allowing officers to not only access call records but also telephone location data.

Conclusion and discussion: towards a threat model for regional journalism

While many journalists may be correct in assuming that they are not a direct target of police, public bodies, intelligence agencies, hackers or spammers, it is evident that no systematic threat modelling has been undertaken by regional newspaper publishers to help journalists arrive at an informed conclusion on the need for information security (RQ1) and as a result few meaningful changes have been made to workflow (RQ2).

While the prospect of fighting legal battles may represent a 'chilling effect' in traditional protection of sources (Smolkin 2005), it might be argued that the time involved in establishing proper security procedures can have a similar effect on journalists pursuing stories which require a consideration of source security.

Given the lack of awareness of both legal and technological threats and vulnerabilities, and ongoing developments on both fronts it is important that news organisations implement such a threat model, reflected in computer usage policies, and regularly review this.

This should be combined with a formal policy relating to when protection of sources can realistically be offered. The BBC's editorial guidelines, for example, provide a useful framework based on the potential for sources being identified through visual and other 'metadata' (RQ3): "We must ensure when we promise anonymity that we are in a position to honour it … When anonymity is essential, no document, computer file, or other record should identify a contributor or source." (BBC 2015)

The broader trend appears to be increasingly turning towards legal systems to control online activity (Freedom House 2014). Meanwhile, technological and commercial developments point to an ongoing increase in the monitoring of people's behaviour which is likely to impact on journalists and their sources. RFID tags, for example (used in staff ID tags and passes, allowing the tracking of movement within a building) were used by the Justice Department to establish contact between an employee and a reporter (Lashmar, unpublished), while event data recorders (EDR - 'black boxes' installed in cars to record details about what the vehicle is doing) have been used by law enforcement without warrant (Abelson, Ledeen and Lewis 2008), and 'wearable technology' such as the FitBit were used for the first time in a Canadian court of law in 2014 (Crawford et al 2015).

On July 30 2015 The Register reported that facial recognition had been used by a UK police force at a music festival. The technology is already increasingly installed as part of CCTV software. And automatic numberplate recognition (ANPR) software which allows authorities to track the movements of individuals has longed formed a part of CCTV infrastructure in the UK (Bridle 2013).

Although the focus of documents such as the IOCCO report has been the use of RIPA by police forces within the last three years, it is important to note that other bodies also regularly exercise their rights under RIPA to access communications data, including intelligence services, HMRC; the Home Office; the Royal Mail Group; Department of Transport; DWP; Charity Commission and local authorities (Interception of Communication Commissioner's Office 2015b, Annex A).

Interviewees felt that local authorities were too cash-strapped to exercise these powers. But 95 local authorities used their powers under RIPA to acquire communications data in 2014, and a further 160 had used their powers in previous years (Interception of Communication Commissioner's Office 2015b Annex A). It is not known how many have used the Act with regard to disclosure of information to journalists which they may classify, as police forces "commonly" did, under "misconduct in public office, a breach of data protection or an offence under the computer misuse act." (Interception of Communication Commissioner's Office 2015, 29). Following the amendments to RIPA regarding journalistic sources, the IOCCO also expressed concern that "it is not clear what authorisation route would be taken by public authorities who do not have powers under the Police and Criminal Evidence Act 1984." (Interception of Communication Commissioner's Office 2015c).

An increasing 'panspectron' or 'surveillant assemblage' where "information is collected about everything and everyone *all of the time* [and whose] main directive is to transform the body into virtual bytes of information - data doubles [of the subject]" (Leistert 2008, 932) represents an important challenge for journalists' ability to address the management of news by media relations and issues of trust in the media, as does employers' rights to read what is sent through company email (Abelson, Ledeen and Lewis 2008; Zureik 2003).

More research is needed on the use of RIPA and access to employees' emails not only by public authorities but also by private companies which increasingly come under the 'watchdog' remit of journalists, as well as the information security practices in parts of the media other than the regional press, including advocacy reporting (Charles 2013).

In addition, the findings suggest that the impact of employer, state and commercial data retention on source relations could be an important and neglected element in research on sourcing practice.

References

Abelson, Hal, and Ledeen, Ken, and Lewis, Harry. *Blown to Bits*, Boston: Pearson, 2008

Ahmad, Shahzad, and Hussain, Furhan. "Snowden Era Challenges: The Story of Surveillance in Pakistan" Paper presented at Surveillance and Citizenship: State-Media-Citizen Relations after the Snowden Leaks. Cardiff University, UK, June 2015

Anderson, David Q.C. "UK INDEPENDENT REVIEWER OF TERRORISM LEGISLATION CRITICISES TOO-BROAD DEFINITION OF TERRORISM." *Independent Reviewer of Terrorism Legislation*. July 22 2014 https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2014/07/22-July-2014-PRESS-RELEASE.pdf

Anderson, David Q.C. "THE TERRORISM ACTS IN 2011." *The Stationery Office*. June 2012. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/228552/9780108511769.pdf

Backman, Johnson and Saetnan, Toendel and Svenonius, Yngvesson.'Post-Snowden Surveillance Journalism in Scandinavia." Paper presented at Surveillance and Citizenship: State-Media-Citizen Relations after the Snowden Leaks. Cardiff University, UK, June 2015

Bakir, Vian. "News, Agenda Building and Intelligence Agencies: A Systematic Review of the Field from the Discipline of Journalism, Media and Communications." *The International Journal of Press/Politics*, *20*(2) (2015): 131-144.

Bates, Stephen "The reporter's privilege, then and now." *Harvard University: The Joan Shorenstein Center on the Press, Politics and Public Policy*. Research paper R-23, April 2000. http://shorensteincenter.org/wp-content/uploads/2012/03/r23_bates.pdf

BBC "Section 6: Fairness, Contributors and Consent: Anonymity." *BBC Editorial Guidelines.* Accessed 2015 http://www.bbc.co.uk/editorialguidelines/page/guidelines-fairness-anonymity/

Bertrand, Ina and Hughes, Peter. *Media Research Methods: Audiences, Institutions, Texts*. New York: Palgrave Macmillan, 2005

Brake, David R. *Sharing Our Lives Online*, Hampshire: Palgrave Macmillan: 2014

Brand, Robert. "Between privilege and subpoena: the protection of journalists' confidential sources." *Ecquid Novi African Media Studies 27(2)* (2006) 111 – 134

Bridle, J. "How Britain Exported Next-Generation Surveillance." *Matter*. December 18, 2013 https://medium.com/matter/how-britain-exported-next-generation-surveillance-d15b5801b79e

Bromium Labs. "Endpoint Exploitation Trends 1H 2015." 2015 https://www.bromium.com/sites/default/files/rpt-threat-report-1h2015-us-en.pdf

Bryman, Alan. *Social Research Methods*, Oxford: Oxford University Press, 2001

Carlo, Silkie and Kamphuis, Arjen. *Information Security for Journalists*, London: CIJ: 2014

Carlson, Matt. "Whither anonymity? Journalism and Unnamed Sources in a Changing Media Environment." In *Journalists, Sources, and Credibility: New Perspectives* edited by Bob Franklin and Matt Carlson, 37-48. London: Routledge, 2011

Charles, Mathew. "News, Documentary and Advocacy Journalism." In *Journalism: New Challenges* edited by Karen Fowler-Watt and Stuart Allen, 384-392. Bournemouth University: Centre for Journalism and Communication Research, 2013

Cheng Daisy Xiaoxuan and Lee, Francis L. F. "Journalist-Source Relations." *Journalism Studies 16(6)* (2015): *850-867*

Crawford, Kate and Lingel, Jessa and Karppi, Tero. "Our metrics, ourselves: A hundred years of self-tracking from the weight scale to the wrist wearable device." *European Journal of Cultural Studies 18(4-5)* (2015): 479-496

Dawes, Simon. "Press Freedom, Privacy and the Public Sphere." *Journalism Studies, 15(1)* (2013): 17-32

Easterby-Smith, Mark and Thorpe Richard and Lowe, Andy. *Management Research: An Introduction*. London: Sage, 1998

Economist. The leaky corporation, Feb 24 2011, http://www.economist.com/node/18226961

EWHC 2092 (Admin) "Case No: CO/3665/2014, CO/3667/2014, CO/3794/2014." https://www.judiciary.gov.uk/wp-content/uploads/2015/07/davis_judgment.pdf

Farr, Charles. "Witness statement, Statement no.1, Exhibit CF1, Case IPT/13/92/CH." *Investigatory Powers Tribunal*. 2014 https://www.liberty-human-rights.org.uk/sites/default/files/Witness%20statement%20of%20Charles%20Farr%20on%20behalf%20of%20the%20Intelligence%20Services%2016th%20May%202014.pdf

Firmstone, Julie & Coleman, Stephen. "The changing role of the local news media in enabling citizens to engage in local democracies." *Journalism Practice*, *8*(5), (2014): 596-606.

Flacks, Richard. "The Question of Relevance in Social Movement Studies". In *Rhyming Hope and History: Activists, Academics, and Social Movement Scholarship* edited by David Croteau, William Hoynes, and Charlotte Ryan, 3-19. Minneapolis: The University of Minnesota Press, 2005

Franklin, Bob & Carlson, Matt. *Journalists, Sources, and Credibility*. Oxon: Routledge, 2011

Freedom House. "Freedom on the Net 2014." 2014 https://freedomhouse.org/sites/default/files/FOTN_2014_Full_Report_compressedv2_0.pdf

Goodwin v United Kingdom. "22 EHRR 123." 1996 *European Court of Human Rights*. Retrieved from http://hudoc.echr.coe.int/eng?i=001-60596

Greenberg, Andy. *This Machine Kills Secrets*. London: Virgin Books, 2012

Haim, Mario. 'Resetting the Agenda? NSA Coverage in Traditional and New Online Media." Paper presented at Surveillance and Citizenship: State-Media-Citizen Relations after the Snowden Leaks. Cardiff University, UK, June 2015

Henruchsen, , Jennifer R. and Betz, Michelle & Lisosky, Joanne M. "Building Digital Safety for Journalism: A survey of selected issues. *UNESCO*." 2015 http://unesdoc.unesco.org/images/0023/002323/232358e.pdf

Home Office. "Acquisition and Disclosure of Communications Data DRAFT Code of Practice." 2015 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/409562/Acquisition_and_Disclosure_of_Communications_Data_Code_of_Practice__web_....pdf

Independent Press Standards Organisation. "Editors' Code of Practice." 2015 https://www.ipso.co.uk/IPSO/cop.html

Interception of Communication Commissioner's Office. "IOCCO inquiry into the use of Chapter 2 of Part 1 of the Regulation of Investigatory Powers Act (RIPA) to identify journalistic sources." 2015 http://www.iocco-uk.info/docs/IOCCO%20Communications%20Data%20Journalist%20Inquiry%20Report%204Feb15.pdf

Interception of Communication Commissioner's Office. "2014 Annual Report." 2015 http://www.iocco-uk.info/docs/IOCCO%20Report%20March%202015%20(Web).pdf

Interception of Communication Commissioner's Office. "Half-yearly report of the Interception of Communications Commissioner." 2015 http://www.iocco-uk.info/docs/2015%20Half-yearly%20report%20(web%20version).pdf

Kleberg, Carl. F. "The Death of Source Protection? Protecting journalists' sources in a post-Snowden age." London School of Economics, 2015. http://www.lse.ac.uk/media@lse/documents/Death-of-Source-Protection-Carl-Fridh-Kleberg.pdf

Kreiner, Kristian & Mouritsen, Jan. "The Analytical Interview. Relevance beyond Reflexivity". In *The Art Of Science*, edited by Stefan Tengblad, Rolf Solli and Barbara Czarniawska, Malmo: Liver, 2005

Lashmar, Paul. "The 'Five Eyes' are watching you: A new paradigm in the relationship between journalists and sources in the age of meta data." Unpublished, Brunel University

Lee, William E. "Deep Background: Journalists, Sources, and the Perils of Leaking". *American University Law Review 57 (5)* (1998): *1454-1508*

Leistert, Oliver. “Data Retention in the European Union: When a Call Returns”. *International Journal of Communication 2* (2008)

Lewicki, R. J. & Brinsfield, C. T. “Trust, distrust and building social capital.” In *Social Capital: Reaching Out, Reaching In*, edited by Viva Ona Bartkus and James H. Davis, 275-303. Cheltenham: Edward Elgar Publishing, 2009

Lubbers, Eveline. *Secret Manoeuvres in the Dark*. London: Pluto Press, 2012

Malmelin, Nando and Villi, Mikko “Audience Community as a Strategy Resource in Media Work”. *Journalism Practice,* (2015) *1–19. doi:10.1080/17512786.2015.1036903*

Marsden, Chris. “Open letter UK legal academics #drip.” *Slideshare*. 2014 http://www.slideshare.net/EXCCELessex/open-letter-uk-legal-academics-drip accessed May 11 2015

Marsh, Kevin. “Investigative journalism: salience, sources and storytelling”. In *Journalism: New Challenges* edited by Karen Fowler-Watt and Stuart Allen, 222-242. Bournemouth University: Centre for Journalism and Communication Research, 2013

Matthews, Jamie. “Journalists and their sources: The twin challenges of diversity and verification.” In *Journalism: New Challenges* edited by Karen Fowler-Watt and Stuart Allen, 242-258. Bournemouth University: Centre for Journalism and Communication Research, 2013

McNair, Brian. *The Sociology of Journalism*. London: Arnold, 1998

McNair, Brian. “Journalism and Democracy.” In *The handbook of journalism studies* edited by Karin Wahl-Jorgensen and Thomas Hanitzsch, 237-249. Routledge, 2009

Metropolitan Police. “Operation Alice: Closing Report.” 2014 http://www.iocco-uk.info/docs/Met%20Operation%20Alice%20Closing%20Report.pdf

Milan, Stefania. “The Ethics of Social Movement Research.” In *Methodological Practices in Social Movement Research* edited by Donatella Della Porta, 446-464. Oxford: Oxford University Press, 2014

Mols, Anouk. “Not Interesting Enough to be Followed by the NSA': A Frame Analysis of the Dutch Public Debate About the NSA Revelations.” Paper presented at Surveillance and Citizenship: State-Media-Citizen Relations after the Snowden Leaks. Cardiff University, UK, June 2015Morozov, Evgeny. *The Net Delusion*. London: Allen Lane, 2011

Near, Janet & Miceli, Marcia. “Whistleblowing: Myth and Reality.” *Journal of Management, 22*(3) (1996) 507-526

O’Neill, Deirdre. & O’Connor, Catherine. “The Passive Journalist: How sources dominate local news.” *Journalism Practice, 2(3)* (2008)

Penrod, Grant. “A problem of interpretation.” *The News Media & The Law,* Vol. 28, No. 4 (2004): 4 http://www.rcfp.org/browse-media-law-resources/news-media-law/news-media-and-law-fall-2004/problem-interpretation

Pew Research Center & Tow Center for Digital Journalism. “Investigative Journalists and Digital Security.” February 5 2015 http://www.journalism.org/files/2015/02/PJ_InvestigativeJournalists_0205152.pdf

Price, G. “Wi-Fi Can Be Dangerous: Three Ways To Avoid Getting Hacked.” *Global Investigative Journalism Network*. February 28 2016. http://gijn.org/2016/02/28/wi-fi-users-three-essential-ways-to-avoid-getting-hacked/

Smolkin, R. “Under Fire.” *American Journalism Review*. (2005) Retrieved from http://ajrarchive.org/Article.asp?id=3810

Spaulding, Stacy. “Off the blacklist, but still a target.” *Journalism Studies 10:6,* (2009): 789-804

Theoharris, Athan. “The FBI and the American Legion Contact Program, 1940-1966.” *Political Science Quarterly 100(2),* (1985): 271-86

Van Leuven, Sarah and Deprez, Annelore and Raeymaeckers, Karin. “Networking or Not Working? A comparison of Arab Spring coverage in Belgian newspapers and TV news.” *Journalism Practice 8(5)* (2014)

Vodafone. "Law Enforcement Disclosure Report." 2014 http://www.vodafone.com/content/sustainabilityreport/2014/index/operating_responsibly/privacy_and_security/law_enforcement.html#eocp

Williams, Harte and Turner "Filling the news hole? UK community journalism and the Crisis in Local Journalism." In *Local Journalism: the decline of newspapers and the rise of digital media*, edited by Rasmus Kleis Nielsen, Reuters Institute for the Study of Journalism, 2015. https://reutersinstitute.politics.ox.ac.uk/sites/default/files/Local%20Journalism%20-%20the%20decline%20of%20newspapers%20and%20the%20rise%20of%20digital%20media_0.pdf

Zureik, Elia. "Theorizing surveillance: the case of the workplace." In *Surveillance as Social Sorting*, edited by David Lyon, New York: Routledge, 2003