Digital Journalism

Routledge
Taylor & Francis Group

ISSN: 2167-0811 (Print) 2167-082X (Online) Journal homepage: https://www.tandfonline.com/loi/rdij20

The Information Security Cultures of Journalism

Masashi Crete-Nishihata, Joshua Oliver, Christopher Parsons, Dawn Walker, Lokman Tsui & Ronald Deibert

To cite this article: Masashi Crete-Nishihata, Joshua Oliver, Christopher Parsons, Dawn Walker, Lokman Tsui & Ronald Deibert (2020): The Information Security Cultures of Journalism, Digital Journalism, DOI: 10.1080/21670811.2020.1777882

To link to this article: https://doi.org/10.1080/21670811.2020.1777882

Published online: 25 Jun 2020.

DIGITAL JOURNALISM
https://doi.org/10.1080/21670811.2020.1777882

Routledge
Taylor & Francis Group

ORIGINAL ARTICLE

OPEN ACCESS Check for updates

The Information Security Cultures of Journalism

Masashi Crete-Nishihata[a], Joshua Oliver[a], Christopher Parsons[a], Dawn Walker[a], Lokman Tsui[b] and Ronald Deibert[a]

[a]University of Toronto, Toronto, Ontario, Canada; [b]Chinese University of Hong Kong, New Territories, Hong Kong

ABSTRACT

This article is an exploratory study of the influence of beat and employment status on the information security culture of journalism (security-related values, mental models, and practices that are shared across the profession). The study is based on semi-structured interviews with 16 journalists based in Canada in staff or freelance positions working on investigative or non-investigative beats. We find that journalism has a multitude of security cultures that are influenced by beat and employment status. The perceived need for information security is tied to perceptions of sensitivity for a particular story or source. Beat affects how journalists perceive and experience information security threats. Investigative journalists are concerned with surveillance and legal threats from state actors including law enforcement and intelligence agencies. Non-investigative journalists are more concerned with surveillance, harassment, and legal actions from companies or individuals. Employment status influences the perceived ability of journalists to effectively implement information security. Based on these results we discuss how journalists and news organisations can develop effective security cultures and raise information security standards.

KEYWORDS

Information security; freelance; beat; security culture

Introduction

Protecting sources and confidential information is an ethical duty for journalists. Information and communications technologies introduce threats that can challenge this responsibility (Schulz and Belair-Gagnon 2018). A recent UNESCO study on source protection calls for legal source protection to be extended to all acts of journalism including digital reporting and communications (Posetti 2017). Numerous cases have emerged of digital surveillance targeting journalists and newsrooms that can jeopardise source protection and the safety of journalists (Wagstaff 2014; Perlroth 2013; Timberg 2013; Scott-Railton et al. 2017). However, despite growing documentation of these types of incidents and the rising calls for journalists to develop proficiency in information security (Horsley and OSCE 2014; Henrichsen, Betz, and Lisosky 2015),

CONTACT Masashi Crete-Nishihata masashi@citizenlab.ca

studies into how journalists perceive and practice information security are limited (McGregor et al. 2015; McGregor, Roesner, and Caine 2016; McGregor and Watkins 2016; Watkins et al. 2017; Pew Research Center 2015; Shelton 2015; Tsui 2019). Addressing this research gap requires mapping the "security culture" of journalism, defined as security related values, mental models, and practices that are shared within an organisation or across a profession (Karlsson, Astrom, and Karlsson 2015). Security culture is a vital part of ensuring members of a group understand, follow, and implement security practices and policies (Karlsson, Astrom, and Karlsson 2015; Hu et al. 2012; Thomson, von Solms, and Louw 2006).

This article provides a case study that explores the information security culture of journalism and analyses the influence of beat (i.e., the subjects and institutions that journalists are assigned to report on) and employment status (i.e., staff journalist or freelancer). The study is based on semi-structured interviews with 16 journalists in Canada working in either staff or freelance positions who self-identified as reporting on investigative or non-investigative beats.

Studies have shown that while journalists share core norms and practices, they experience journalism in diverse ways depending on their political economic, social, and cultural context (Hanitzsch et al. 2019). We concentrate on beat and employment status because these variables are strong influences on the general professional cultures of journalism (Bennett 1990; Gollmitzer 2014; Walters, Warren, and Dobbie 2006; Cohen 2016), but no research has focussed on their impact on security culture. Overall, our results show that security culture in journalism is not uniform resulting in a range of approaches that are influenced by beat and employment status. We find that the values and norms developed through beat and employment status are a stronger basis for security culture than policies set by media organisations. If institutional rules come into conflict with these norms and values journalists will follow their own practices.

At the root of these various security cultures are mental models of security differentiated by beat. The perceived need for information security is tied to how journalists assess the "sensitivity" of a particular story or source. All the investigative reporters in our study considered some aspect of their reporting to be sensitive. Journalists in our study who were exposed to investigative work had greater familiarity with information security tools and practices. By contrast, non-investigative journalists we interviewed who did not consider their work to be sensitive did not see a need to practice information security. These findings echo previous research from McGregor et al., who similarly observed a "security by obscurity" mindset in which journalists only view information security as necessary when they are working on stories that are sufficiently sensitive to attract the attention of government authorities (McGregor et al. 2015).

While this mindset appears to be common, information security is not only an issue for investigative journalists. Reporters across beats express concern over a range of security threats. Investigative journalists are concerned with surveillance and legal threats from state actors including law enforcement and intelligence agencies. Non-investigative journalists are more concerned with surveillance, harassment, and legal actions from companies or individuals. The range of threats described by journalists from across different beats shows that keeping information secure from state actors is only one model of security that is at the extreme end of a spectrum of risks.

Employment status influences the ability of journalists to effectively implement information security. Journalists describe employment status as presenting contrasting capacities and constraints that have to be navigated as they try to integrate information security into their workflow. Staff reporters have greater access to resources, but struggle with autonomy over information security systems and decisions. In contrast, freelancers have greater autonomy but are hindered by lack of resources.

The article proceeds as follows: in the Literature Review section we review studies on security culture, information security for journalists, and the influence of beat and employment status on professional culture; The Methods section describes our method; The Results section reports our findings; The Discussion section discusses the implications of our results and steps that journalists and news organisations can take to foster effective security cultures and raise information security standards; Finally, we conclude with an outline of future work.

Literature Review

In this section we review literature on journalism culture, security culture, the security practices and perceptions of journalists, the general influence of beat and employment status on journalism, and background context for our case study. Based on this review we conclude that our study should consider institutional and professional influences on security culture and that beat and employment status are important variables to include in our analysis.

Journalism Culture

The World of Journalism project is the largest comparative study of journalism surveying journalists from sixty-seven different countries. A core finding of the study is that while journalists share some basic professional norms and practices they may experience the profession in significantly different ways depending on their political, economic, social, and cultural context (Hanitzsch et al. 2019). There is no single journalism culture but a multitude of cultures that can be expressed in different sets of ideas and values, practice of news production, and outputs of news content. While the World of Journalism project and related studies on journalism culture cover a wide range of variables none of these studies include analysis of how journalists approach information security. To help inform our analysis we review research on security culture from organisational studies.

Security Culture

Organisational studies scholars have recognised security culture as one of the most important influences on the information security behaviour of individuals (Karlsson, Astrom, and Karlsson 2015; Hu et al. 2012; Thomson, von Solms, and Louw 2006). Although studies have offered different definitions, a critical literature review by Karlsson found a common understanding that security culture "consists of a shared pattern of values, mental models and activities that are traded among an

organisation's employees over time, affecting information security." (Karlsson, Astrom, and Karlsson 2015)

This definition reflects the fact that much of the research into security culture has focussed on its effect on employees' behaviour in an organisational context. However, security culture can also transcend organisations and differences in culture can be observed between professions. Two studies in particular build on the general consensus in professional culture research that professions have cultural differences to argue that similar differences exist in the field of information security (Ramachandran, Rao, and Goles 2008; Ramachandran et al. 2013). Ramachandran, Rao, and Goles (2008) observed differences in the security culture between workers in four professions: accountancy, information systems, human resources, and marketing. Notably, one point of difference between the professions was the extent to which security culture derived from organisational or professional sources (e.g., internal policy or training vs. professional associations or publications). With these concepts in mind we turn to review previous work on how journalists perceive and practice information security and identify gaps in the literature.

Journalism and Information Security

The Snowden disclosures highlighted the need for information security for journalists both in terms of the scope of government surveillance they revealed and by showing that Glen Greenwald nearly missed the story of his career by not having secure tools properly setup to receive messages from his now famous source (Greenwald 2014). However, a survey study by the Pew Research Centre on investigative journalists found that years after the disclosures were published the information security habits of investigative journalists remained largely the same (Pew Research Center 2015). The majority of journalists surveyed (80%) believe that being a journalist increases the likelihood that their data will be collected by the U.S. government. But half of the journalists did not use any secure tools in their work and only 38% changed how they communicate with sources following the Snowden disclosures (Pew Research Center 2015). These results show a disconnect between how journalists perceive and practice information security.

A number of qualitative case studies further probe the information security practices and perceptions of journalists (McGregor et al. 2015; McGregor, Roesner, and Caine 2016; McGregor and Watkins 2016; Watkins et al. 2017; Shelton 2015; Tsui 2019; Henrichsen 2020). These studies primarily focus on staff journalists from US-based media organisations (Shelton 2015; Henrichsen 2020) with the exception of a series of papers (Mcgregor et al. 2015; McGregor, Roesner, and Caine 2016; McGregor and Watkins 2016; Watkins et al. 2017) that analysed a sample of staff journalists based in the US and France (the location of journalists was not treated as a significant variable), and a study on journalists who report in Hong Kong or mainland China, which found that the location of reporting is an important variable to consider (Tsui 2019).

These studies shed some light on the mindsets of journalists regarding security. A mental model is a simplified conceptualisation for how something operates in reality (Morgan et al. 2001). When applied to security, a mental model or mindset can be

understood as how an individual perceives and conceptualises security risks and makes decisions about them (Asgharpour, Liu, and Camp 2007). McGregor et al., apply a mental model framework to explore what motivates journalists to adopt information security tools and practices, and find that perceived sensitivity of sources and stories was a primary influence (McGregor and Watkins 2016). In another study based on interviews of US-based journalists and security trainers, Henrichsen similarly found the security by obscurity mindset was an obstacle to adoption of secure tools and practices (Henrichsen 2020). Tsui and Lee expand on the framework presented by McGregor and Watkins (2016), and identify threat awareness (knowledge of potential threats) and protection awareness (knowledge of techniques to defend against threats) as indicators for three levels of security mindsets: "security by obscurity" (low to medium threat awareness and low protection awareness), "security by obfuscation" (medium to high threat awareness and medium protection awareness), and "security by opportunity" (high threat awareness and high protection awareness) (Tsui 2019).

Within news organisations, journalists are typically treated as autonomous peers rather than subordinates. This autonomy creates challenges for introducing and enforcing security policies (McGregor, Roesner, and Caine 2016), which managers perceive as one of the most important tools for shaping organisational security culture (Van Niekerk and Solms 2010). Journalists, editors, and technical staff may also conceptualise and prioritise security issues differently, to the effect that reporters may resist and resent top down efforts to change security practices, or may see security as important, but struggle to get institutional support towards its implementation (McGregor, Roesner, and Caine 2016). Henrichsen's study found that a general lack of security culture in journalism and conflict between journalists and IT professionals within news organisations are among the key barriers to journalists adopting information security technologies (Henrichsen 2020). Watkins et al., found that it was common for the journalists in their study to seek information security support and advice from contacts outside of their organisation, which creates guidance that managers cannot evaluate or control (Watkins et al. 2017). The challenge identified by Watkins *et al,* presumably is heightened given that an increasingly large portion of the news is produced by freelancers (Drohan 2017), who do not fall entirely within the culture of any organisation and therefore likely have employment conditions that differ considerably from those of staff reporters.

Based on the literature we conclude that an organisational frame is insufficient for understanding security culture in journalism, due to multiple external influences that shape culture outside of institutions including the individual mindsets of reporters, their sources, and their peer networks (McGregor et al. 2015; McGregor, Roesner, and Caine 2016; McGregor and Watkins 2016; Watkins et al. 2017). Studies of journalism culture further show that there are multiple experiences and interpretations of culture in the profession (Hanitzsch et al. 2019). To probe how journalists may experience information security differently our study explores two sources of potential influence on security culture: institutional, and professional. Understanding how security culture may be influenced by professional norms and values requires insights into the general professional culture of journalism. Previous work has shown that beat and employment status can significantly shape how journalists perceive and carry out their work.

Influence of Beat

"Beats" – the systematic division of subjects and institutions that journalists are tasked with covering – are an important structural feature of journalism. Beats influence how journalists process events into news (Schudson 1989), how they interact with their competitors (Grey 1966), and their perceptions of professional status (Schiller 1979). Beats have also been described as a "social structure" of journalism, that facilitates the transmissionof professional norms (Bennett 1990). Together with previous studies on journalism and information security, these conceptions of beat suggest that different beats may affect how journalists think about security, how they practice it, and how they communicate and learn about it amongst themselves.

Influence of Employment Status

Freelance journalists are self-employed and typically sell their services to multiple outlets without long-term commitments and sometimes with only verbal agreements. Freelancers also often receive less remuneration for their labour compared to their staff colleagues (Ladendorf 2013). Furthermore, the economic situation for freelance journalists is usually more perilous, because they lack job security and have limited access to benefits (Gollmitzer 2014; Nies and Pedersini 2003; Walters, Warren, and Dobbie 2006; Cohen 2016; Professional Writers Association of Canada, 2006).

A relative lack of institutional support when compared to staff journalists can potentially introduce significant legal and physical safety risks for freelancers. For example, freelancers frequently do not have insurance or access to legal protection in the event of a defamation claim based on their journalism (Lee-Wright 2012). This reality, as well as economic considerations, can dissuade freelancers from pursuing investigative reporting that may pose legal threats (Walters, Warren, and Dobbie 2006). In hostile environments such as conflict zones, freelancers often operate without safety insurance, appropriate training, or equipment and, simultaneously, may be motivated to take on risky stories to get work (Mahoney 2015).

Despite these challenges freelancers describe their status as providing independence and autonomy that is distinct from staff roles, such as control over work schedules and the flexibility to engage in stories of professional and personal interest (Mathisen 2017). Studies have found that freelancers regard themselves as highly professional and describe independence and autonomy as major contributors to their overall job satisfaction (Gollmitzer 2014; Das 2007; Edstrom and Ladendorf 2012). However, the reality of freelance work may be more constrained than freelancers say. Due to their precarious economic position, freelancers have little choice but to meet their clients' expectations, which may compromise their independence in practice (Das 2007). Indeed, some freelancers describe the discussion of autonomy as a self-propagated myth to help make them feel better about their work (Edstrom and Ladendorf 2012).

Based on these studies, we determine that examination of security culture in journalism should take account of freelancers as linked to but not fully part of organisational security cultures, and as potentially experiencing different capacities and constraints than their staff colleagues.

Case Study Background

We situate our analysis in Canada, which reflects typical media conditions in Western countries. Canada has a robust and free press, media includes a diverse range of journalistic beats including investigative and non-investigative areas, economic constraints have increased media institutions' reliance on freelancers, and there are recent cases of government authorities targeting journalists because of their work (Cohen 2016; Drohan 2017; Reporters Without Borders 2017).

Canada has a high concentration of media ownership. Four companies control roughly 80% of the television and newspaper industries in Canada; although Internet news is less concentrated, nearly 50% of online news is supplied by just eight outlets (Winseck 2016; Standing Senate Committee on Transport and Communications 2006; Standing Committee on Canadian Heritage 2017). In the past decade, newspaper publishers in Canada have seen their revenues drop significantly and consequently have closed news outlets and reduced the number of employed journalists (Drohan 2017; Standing Committee on Canadian Heritage 2017). As staffing levels decline, full-time positions have often been replaced by freelance and contract workers, and existing full-time staff are placed under increasing pressure to produce more news on more platforms (Drohan 2017). The economic pressures in Canadian newsrooms were captured in the 2012-16 Worlds of Journalism Study, in which three-quarters of Canadian respondents reported increasing demands to make profits, longer working hours, and less to time to work on each story (Worlds of Journalism 2016).

Reporters Without Borders lowered Canada's rank in the World Press Freedom Index from eighth most free country globally in 2015 to twenty-second in 2017, its lowest rank since the Index began in 2011 (Reporters Without Borders 2017). This decline is associated with a series of events affecting journalists. First in 2015, the Royal Canadian Mounted Police ordered a journalist working for VICE News to hand over records of all communications with a source who was suspected of joining the terrorist group ISIS (Canadian Journalists for Free Expression 2017). In Quebec, seven journalists were subjected to police surveillance in two separate cases, where authorities had sought out journalists' confidential sources inside the province's police force (CBC 2016). These recent cases increase the salience of information security for journalists in Canada insofar as domestic state surveillance and legal tools have been used to subvert journalist-source confidentiality.

Methods

In this section we describe our interview method, data coding and analysis approach, participant recruitment, research ethics, and study limitations.

Interview Method

As there is no prior work on security culture of journalism that systematically evaluates the influence of beat and employment status, using qualitative semi-structured interviews is an appropriate method for an exploratory study. Our interview guide was designed to elicit details on how journalists conducted their work and their experience

Table 1. Participant demographics.

	Investigative	Non-investigative	Total
Staff	3	6	9
Freelance	3	4	7

and perception of information security with a focus on three major questions: how journalists deal with sensitive information; how journalists communicate with sources; and which threats to news making journalists perceive or experience. The interview questions were open-ended and avoided explicitly asking about information security to reduce the introduction of bias. For example, rather than asking "do you use secure tools to communicate with sources"? we asked "do you do anything special to communicate with sources"? If, in response, participants described an information security tool or practice then further probes were used, which were specifically related to information security. See Appendix 1 for a copy of our interview guide.

Participants

Over the course of three periods (in 2015, 2016, and 2017) we conducted semi-structured interviews with 16 journalists who worked in Canada. Participants were primarily selected based on pre-existing relationships between the researchers and journalists, as well as through referrals from these contacts. The majority of the interviews were done in person (two were done over the phone). All interviews were audio recorded and transcribed verbatim. The interviews averaged 79 min in length.

We recruited participants who were either staff journalists (defined as journalists in a full-time salaried position at a media organisation) or freelance journalists (defined as self-employed journalists who sell services to publications). Participants self-identified as working on a variety of journalistic beats and whether they considered their beat to be investigative in nature. One participant served as an editor, and two had experience as television producers. Table 1 shows the distribution of employment status and beats across our participants.

Participants included relatively junior journalists (e.g., under 3 years of experience) to senior reporters (e.g., over 20 years of experience). Participants averaged 11.6 years of experience. Participants worked in a range of mediums including online, print, radio, and video, and primarily for large media organisations (over 100 employees) with the exception of one participant who worked for a small organisation (under 25 employees).

Data Coding and Analysis

We examined the interview transcripts using inductive thematic analysis to identify emergent themes in the data (Herzog, Handke, and Hitters 2019). Using a data driven process, three independent researchers grouped transcripts into codes and conducted regular checks for inter-coder reliability. Data analysis was conducted and managed through the Atlas.ti qualitative analysis software suite. Preliminary data analysis of the codes revealed emergent themes surrounding digital security perceptions and practices that showed differences in the experiences of journalists based on beat and professional

status. Based on this early coding we furthered our data sampling to balance the number of participants from staff and freelance positions and investigative and non-investigative beats. Once we reached saturation in the responses from participants, we did another cycle of data analysis including a review of literature from journalism, security, and organisational studies. Informed by frameworks of security culture we further probed the data to explore the influence of beat and professional status. Following this analysis, we grouped codes into three finalised themes: values and mental models, perception of threat, and security practices (see Appendix 2 for coding samples).

Research Ethics

We received institutional ethics review approval before conducting interviews. Participants were instructed that they could refuse to answer any question they did not feel comfortable responding to and could request that any portion of the interviews be omitted from analysis. We also explained that we would redact any references to the participants' identity and their organisation in interview transcripts and final presentation of results, but we would describe their general professional role (e.g., investigative reporter) and profile of their organisation (e.g., large print-based news organisation). All audio recordings and transcripts were encrypted at rest and stored locally in our research facility. No participants opted to withdraw from the study.

Limitations

Our qualitative study is based on a small sample size (16 participants) and therefore while our results are useful for an exploratory view of the security culture of journalism, they are not generalisable. Although media in Canada is highly concentrated and our sample includes a balanced representation of major national news in the country there are areas relevant to the case study that we were unable to include in our analysis due to time and resource constraints. For example, we did not include French speaking media, which is an important segment to explore given the aforementioned cases of police surveillance against journalists in Quebec. We also did not interview participants who work for aboriginal news outlets who due to their minority status may have greater social vulnerabilities and different security concerns and experiences. At a wider level, we also did not systematically explore potential differences introduced by journalistic medium (e.g., print, radio, video, photography, *etc.*) While we comment on some gender issues that emerged in this study, a direct focus on gender is left for future research. In terms of comparative analysis our results are based on the experiences of journalists in Canada who operate within a generally free press environment. We expect that journalists working in authoritarian countries with greater threats to press freedom are likely to face different challenges leading to different security cultures.

Results

Our analysis focuses on identifying the influence of beat and employment status on security culture through three themes: values and mental models, perceptions of

threat, and security practices. These themes are informed by the definition of security culture in Karlsson's literature review, which identifies values, mental models, and activities affecting information security as the three commonly accepted elements of security culture (Karlsson, Astrom, and Karlsson 2015).

Values and Mental Models

Within this theme we analyse how journalists conceptualise information security and its relationship to professional values and responsibilities. Across beats and employment statuses, journalists share a professional value of protecting sources and confidential information. An editor underlined that if a story is sensitive "*usually the chief concern is protecting the source*." Protecting sources is a value held by the journalists we spoke to but not all of the journalists in our study consider their work to be sensitive.

Perceptions of Sensitivity

Perceptions of story and source sensitivity are key to whether journalists consider information security as a necessary part of their work. We asked participants if they considered any aspect of their reporting to be sensitive. We designed the question to be open-ended and allowed the participants to define "sensitivity" themselves to avoid introducing bias. A freelance investigative journalist explains the spectrum of sensitivity that can be encountered:

> *"Reporting on government in general – especially if you're looking to break stories and you can access government secrets – is by definition sensitive … even when it comes to business reporting, if you're talking about accessing sensitive or proprietary business information, you're potentially putting a target on your back for other folks who might be interested in that information."*

In contrast, non-investigative reporters in our study who do not describe their work as sensitive do not prioritise information security. A staff reporter on a city beat explains:

> *"The work that I do is not necessarily … hard hitting, investigative … kind of Watergate- style journalism … [information security has] just never really come up because it is not something that sources are particularly concerned about vis-à-vis the kindsof stories that I'm writing."*

Similarly, a generalist freelancer said: "*I generally don't do a lot of investigative stuff. I don't do a lot of sensitive stuff. So, protecting information for me is not a high priority*." This perspective is described by McGregor et al., as the "security by obscurity" mindset in which journalists consider the threat of government authorities pressuring sources and journalists as the benchmark for evaluating if information security is required (McGregor and Watkins 2016). According to this mindset, information security threats are primarily an issue for investigative reporters – if a journalist is not doing what they consider to be sensitive investigative work then they do not have to prioritise information security. A freelance non-investigative journalist compared their degree of risk to that of investigative colleagues:

> *"[For] the kind of journalism I am doing now – I don't feel particularly under threat. If I was an investigative journalist, I would have an entirely different perspective on security."*

These results show that participants share a professional value of source protection but diverge in their perception of sensitivity. Investigative journalists are viewed as doing more sensitive work and therefore needing greater attention to information security tools and methods. These mental models reveal different security cultures formed around beat.

Perception of Threats

In this theme we analyse how journalists approach security threats. We categorise the threats they describe into four dimensions:

1. The type of threat (e.g., legal, technical, physical);
2. If the threat was directly experienced by participants (or a colleague), or was perceived as a possible risk;
3. The target of the threat (e.g., organisation, individual journalist, source);
4. The adversary that was involved or suspected to be involved (e.g., law enforcement, companies, individuals, *etc.*)

Our results primarily reflect participants' perceptions of threat and how they conceptualise risk. These perceptions and concerns include digital and non-digital threats to information and vary by the beats that participants cover. Investigative journalists are particularly concerned with surveillance and legal threats from state actors including law enforcement and intelligence agencies. In contrast, non-investigative journalists are more concerned with surveillance, harassment, or legal actions from companies or individuals. Professional status does not appear to affect the types of threats that journalists perceive or experience.

Perceptions of Threats: Investigative Journalists

Investigative journalists in our study consider the threat of state actors targeting them due to their reporting. A staff investigative journalist explains the security concerns that possessing sensitive governmental information can entail:

> *"You might find yourself in possession of a classified document… you may have to contemplate what would happen to you if you crossed the border with the document, or a search warrant in relation to such documents… in some cases you might wonder whether police might want to… tap your communications or at the very least figure out who you're talking to."*

Other journalists discuss the range of state authorities and public institutions that have been or could be threatening, including intelligence agencies, police, and border agents. A staff investigative journalist said "*I have certainly in the course of my work around policing and corruption… been followed. I have had what I believe are my phone calls intercepted. I suspect I've been the target, but I have no hard proof.*"

The investigative journalists we interviewed also consider harassment through questioning by authorities and efforts to identify sources through legal means. A freelance investigative journalist working on a national security beat said, "*I know for a fact that the government has tried to figure out who one of my sources is… from a legal angle.*"

A staff investigative journalist recalled police requesting a full copy of an interview that was only partly broadcast with an individual who was involved in a corporate corruption case, which was the subject of a police investigation. The journalist explained: "*our job isn't to help the police, and so we say no thank you, and they say, "we're going to prepare a production order" … we've had requests, but never been served with a search warrant*."

These investigative journalists share a perception that there is a certain level of sensitivity at which information security becomes more relevant to their work, with a particular focus on government adversaries. This threat model is the benchmark for information security according to the "security by obscurity" mindset (McGregor and Watkins 2016).

Perception of Threats: Non-Investigative Journalists

Non-investigative journalists describe different concerns than investigative reporters, ranging from private companies monitoring sources and threatening libel and defamation to private individuals engaging in online harassment and personal threats. Non-investigative journalists working on business related beats describe threats that reporting on certain business sectors could introduce. For example, journalists note the potential for telecom companies to threaten legal action: "*There's been telecom companies that have threatened [libel charges] … They threatened to sue*." Sources from these industries also require protections:

> "*I cover telecom so the companies themselves are … in a lot of cases pretty vigilant about keeping tabs on their employees' communications. So, it helps … [to] … try to avoid writing anything in any communication that could suggest that they're giving you information that they shouldn't be giving you*."

Harassment from individuals who can be characterised as "angry readers" was highlighted by non-investigative journalists. This harassment typically takes the form of threatening messages. Some cases include the unauthorised distribution of personal information (referred to as "doxing"). A freelance non-investigative journalist recalled an incident following an article they wrote about a video game: "*there was a thread set up online where people were posting my address, my phone number. It was kind of frightening*." A staff non-investigative journalist explained that "*the biggest threat would … probably be doxing … occasionally I'll write stories about men's rights groups or right-wing online groups– kinds of online groups who might be motivated to try to do something*." Concerns over the threat of doxing motivated the journalist to be more vigilant about account security:

> "*I've thought of [doxing], which is why I am also concerned about making sure all my accounts are locked down. I think there is probably enough information out there about me that I am not completely safe, but at least for my own accounts that I can control, I've tried to reduce my visibility*."

Some of the female participants experienced harassment and sexualised threats online, described by one of the staff non-investigative journalists as "*general Twitter harassment and awful little things that happen when you are a woman in a somewhat public life*."

The perceptions and experiences shared by non-investigative journalists show that digital surveillance conducted by state actors is a narrow subset of information security threats that journalists may experience. While non-investigative reporters have less concern with threats from government actors the threats they describe could also have significant consequences.

Security Practices

In this theme we explore the information security practice of journalists. We examine what actions journalists take to protect their information and find that beat and employment status shape these activities. Beat is correlated with differing familiarity and exposure to secure tools and concepts. Employment status strongly influences the capacities and constraints journalists experience in their efforts to engage in secure practices. In our analysis of the influence of employment status on security practices we also observe how a journalists' security culture can come into conflict with the norms and policies of their newsrooms.

Beat and Security Practices

The use of tools to protect digital files and communications was low amongst participants. The investigative journalists in our study had more experience with secure tools than their non-investigative colleagues. The participants in the non-investigative category who had experience with security tools also had prior experience with investigative reporting. These results suggest that exposure to secure tools and concepts is tied to perceived sensitivity of reporting. Journalists working on more "sensitive stories" are more likely to be introduced to secure tools and have greater levels of adoption.

Employment Status and Security Practices

Freelance and staff reporters who work on similar beats and share comparable perceptions of threat describe different practices due to organisational and resource constraints tied to their professional status. Staff journalists have greater access to resources but are constrained by bureaucratic structures and organisational policies. Freelancers, on the other hand, describe greater autonomy but are constrained by lack of resources and institutional support.

Capacities for staff journalists include increased access to resources and institutional support. Greater access to equipment was described as important for supporting information security practices. An investigative reporter with experience as a freelancer and staff journalist explains:

> *"When you work for an institution you theoretically have … budget to get you hardware and stuff that you need … let's say you have a really crappy Android phone as a freelancer, all of a sudden when you're on staff you have leverage to get an iPhone that's more secure."*

Support from trained staff on both legal and technical issues is another perceived benefit of working for an organisation. An investigative journalist with staff and freelance experience described organisational security and IT support as a benefit: "*the pro [of being on staff] is that you obviously have a … security team …. that is responsible*

for managing that information and those systems." For some journalists, however, disconnections between the IT department and inflexible IT policies were described as an annoyance and in some cases as a major obstacle for adopting secure tools and practices. A freelance video journalist with experience in television production described IT staff as being territorial about the use of systems and hindering the ability of journalists to install secure communications applications:

> *"There would be these skirmishes every time somebody wanted to download … Jitsi … Jabber [encrypted chat applications] or whatever, because it would have to go through theIT guys … .I think, [they] saw it as a source of annoyance and … stepping into their territory. It created a lot of friction for a while."*

Some participants resorted to using personal devices and accounts for their work due to frustrations with IT policies. One investigative staff journalist's security practices were shaped by a desire to keep clear of the IT staff:

> *"I view my workplace as a threat … part of the reason why I was … really adamant about using … my own devices … and having a laptop that was largely free from IT is because I was very cognisant of the fact [that] … if I was ever doing something that was super sensitive and was communicating with a PGP [encrypted email] key I didn't want to be in a position where my employer would have access to that PGP key."*

Another institutional constraint was upper management misunderstanding information security and not prioritising it in the organisation: "*I have a large bureaucratic organisation that doesn't prioritise [information security] yet … there are certainly rumblings and people in places of high authority acknowledge it is something we need to look at. But they just … they don't understand it*."

The lack of prioritisation for information security also meant that training on security practices was rarely provided. A reporter (who did not identify as an investigative journalist) said they had participated in formal information security training provided by their institution, due to them being put on a sensitive investigative story. Without this level of institutional support, journalists learn about information security from peers and turn to resources outside of the newsroom. In one case a freelance journalist recalled that in a former role as a television producer they took it upon themselves to engage in independent staff training:

> *"I remember fighting for digital security training early on, like 2010-2011 … in the organisation I was at the time as a producer and being met with like totally blank stares. I think that at various points certain staff sub-groups have argued for it or sort of figured out a way of doing it informally."*

Overall, we see staff journalists across beats enabled by resources and in some cases support staff, but constrained by restrictive policies, lack of training, management misunderstanding security, and disconnects with IT departments. These disconnections reflect fundamental differences in how journalists and institutions conceptualise security culture.

In contrast to staff reporters, freelancers in our study describe having greater autonomy over information security decision making. A freelance investigative journalist explained that they have better control over where data was stored and handled as a freelancer than as a staff reporter:

"Being a staffer, a lot of your information could be held in a different jurisdiction … As a freelancer, you have a lot more freedom to say I'm going to keep this information offline. I'm going to keep this information domestic, local, or I'm going to apply x, y, and z tactic to make sure it's not vulnerable to the outside."

The same journalist also described autonomy over decisions of how to protect sources as a capacity derived from their employment status:

"Being freelance, means if [authorities] show up, I can prefer to go to jail than hand over any information. Whereas an employer doesn't have that luxury. They are looking potentially at the other end of bankruptcy or who knows what. And at the end of the day their responsibility is not to my source, their responsibility is to their shareholders, their financiers, or the rest of their employees. Being self-employed I have the freedom to continue to say "no" to fight against any production order or subpoena that may arise, which is good."

The most serious constraints for freelancers are lack of resources and institutional backing. Lack of legal protection left freelancers vulnerable particularly if they worked on sensitive topics: "*You don't necessarily have the same legal protection either way when you're a freelancer … that can play a role – especially when you're trying to kind of poke at things that might have national security implications or just might be particularly sensitive*."

Limited equipment budgets are also a major impediment for freelancers adopting information security. A freelance video reporter explained:

"I can tell you that it would be better to have a burner phone for travel and an extra laptop. I can also tell you that no freelancer, unless they're literally working on an Edward Snowden-type story, is going to have that as a matter of course, because that is four thousand dollars that they just don't have."

The same journalist noted that lack of access to equipment made it particularly challenging to have autonomy over information security as a freelancer doing video productions:

"The only time that it is potentially helpful [to be freelance] is at the point that you are an independent entity of your own and have gathered enough resources that you can have an edit suite in house and kind of control … every stage of production … in theory that's the point that you can potentially protect the material the most because there is nobody is going to make you ingest it into any system. You own it, not somebody else. But I don't think that happens for most people."

In comparison to staff journalists, freelancers describe greater autonomy over information security since they do not face direct pressures to conform to organisational policies. While, freelancers, relative to staff journalists, may not be encumbered by tensions between professional and institutional security culture, the material cost of news production and lack of institutional support can inhibit their abilities to adopt secure practices.

Discussion

Our results show that journalism lacks a uniform security culture and is fragmented by beat and employment status. In this section we describe the implications of our findings for journalists and news organisations.

Security Culture Fragmented by Beat

Beat strongly influences how journalists perceive and value information security. We find a divide between investigative and non-investigative reporters that echoes previous research (McGregor and Watkins 2016; Henrichsen 2020) and shows that journalists view information security as only necessary for those working on sensitive stories that could attract the attention of government authorities. While the journalists we interviewed agree that source protection is a professional obligation, information security was seen as a more necessary precaution for investigative journalists.

The need for information security practices to protect sources may be more obvious in investigative journalism. However, there are many reasons to challenge the perception than information security is only relevant to certain beats or stories. First, this attitude can be an excuse for disregarding information security in other types of journalism. The range of threats our participants described suggests that basic security awareness and practices are warranted for all journalists. Second, journalists who view information security as only a concern for investigative colleagues may fail to understand the effects of their own actions on those colleagues. For example, an investigative reporter explains that newsrooms and journalists need to see how individual actions can impact the wider organisation:

> *"you've amassed a team of people any one of whom could be a weak link. Your information could only be as protected as… you know, when your co-workers want it to be protected – especially when you're working in a company where not everyone is a journalist or not everyone is practising good cybersecurity… your whole system could be vulnerable."*

Third, beats are fluid. Journalism lacks a widely accepted definition of "investigative journalist". Journalists covering non-investigative beats also reported dealing with some sensitive stories and sources. A journalist covering any beat could potentially uncover a sensitive story or source that would require greater attention to security. For example, a sports reporter may learn of a doping scandal or a city journalist may uncover municipal corruption. In such scenarios, journalists in seemingly "non-sensitive" beats have just become investigative reporters. For these reasons the mentality that information security is only applicable to investigative journalists can professionally limit the ability of non-investigative journalists to protect sources and effectively and safely report news while also potentially putting other colleagues at risk.

Bridging the Divide between Staff and Freelance Reporters

Employment status effects the ability of journalists to implement information security. Staff journalists have the advantage of resources and institutional backing but are encumbered by organisational policy. On the other hand, freelancers have the advantage of autonomy but suffer from resource constraints. Staff journalists who are actively trying to be more secure may find that their organisations do not share the same values, mindsets, or practices as them, which creates distrust and inefficiencies. In some cases, this tension led journalists to use personal accounts and devices and try to shield their digital assets from their organisation. Others addressed the gap by forming peer-based groups based loosely on beat to support training in information security. These practices indicate that security culture is more influenced by beat and

peers than institutional policies and journalists prioritise the values, mindsets and practices they develop independently.

The gap between institutional and professional security culture is widened for freelancers. Freelancers and staff journalists share professional values and mental models related to information security. However, they differ in their practices and activities. These differences do not arise because of different security needs, but because of employment status, organisational limitations, and resource constraints. Operating outside of formal organisations means that freelancers more strongly identify with security norms, mindsets, and practices formed at the professional level and may require greater peer support (such as training and knowledge transfer often from reporters who work in similar beats).

Media organisations operate with a mix of reporters from across beats and employment statuses. If newsrooms fail to acknowledge the different ways journalists think about security the divides between organisational and professional security culture will continue and challenges for developing effective security policies and ensuring compliance with them will grow.

Towards a more Secure Culture

Our findings inform steps that news organisations and journalists can take to work towards a more security-conscious culture at the professional and institutional level. The ultimate goal for newsrooms should be to equip all journalists regardless of beat or professional status with basic information security awareness and skills, and to tailor more advanced practices and precautions depending on the needs of particular journalists and the threats they face.

Efforts to improve security culture need to address the different ways that journalists perceive and practice security and adopt threat models that acknowledge and address these differences while also finding common norms and values that can unify seemingly disparate approaches to security. McGregor, Roesner, and Caine (2016), found that journalists and stakeholders in news organisations acknowledge the importance of source protection but diverged in information security priorities and practices. An ethnographic study of a newspaper found that when journalists perceive management policies as threatening their autonomy to report news, dissent will increase and policies will be ignored (Ryfe 2009). Our study finds similar issues. When staff journalists feel their autonomy to make good security decisions is undermined by organisational policies they ignore the rules and act independently. Freelancers similarly view the increase in autonomy their professional status provides them as a key benefit. To resolve these tensions journalists and media organisations must recognise the need for information security and nurture a security culture based on the realities of the job that informs policies and practices that are related to norms (such as source protection) that are shared amongst the journalists and other media organisation stakeholders. This prioritisation has to be expressed by news organisations with clear policy and resources dedicated to security. Strengthening information security should be seen as a business opportunity and organisational responsibility that enables better and safer reporting across a newsroom rather than a costly burden only applicable to specialised reporting.

One means for demonstrating the utility of information security is through peer learning and support. In practice, developing strategies for individual journalists to promote and encourage information security amongst themselves and reach beyond colleagues in their beat could help increase security awareness and education. Newsrooms can help encourage this process by providing information security resources and training to all journalists regardless of beat or professional status and defining a baseline level of security for all reporters. Further training and resources should be provided to reporters who may be at higher risk due to more sensitive reporting. Newsroom practices for working with freelancers should also be reviewed to consider how security risks can be minimised in for example how newsrooms and freelance reporters share data.

Developing a baseline level of security and understanding the different threats journalists may encounter requires communication with reporters and development of threat models that are informed by context. As a freelance journalist notes media companies need to take information security: "*seriously as … a real thing that impacts not just the people who they think are doing sensitive reporting. So not just their national security reporters*." Our study shows that journalists from a range of beats face information security threats, but journalists and media institutions place emphasis on the threat models of investigative journalists. By providing baseline training to all journalists and specialised training where necessary newsrooms can avoid silo approaches to security while also recognising the contextual differences between journalists. Overall, moving towards a security culture that acknowledges diversity in how journalists and institutions practice news making while advocating and supporting the utility of information security requires approaching security as a collective effort rather than an individualised practice.

Conclusion

Our study shows that analysis of journalism security culture should consider individual and organisational influences. Through this frame the fragmented security culture of the profession can be surfaced and understood. Our study shows that beat and professional influence how journalists perceive and practice digital security. These findings are from a small exploratory study and are not generalisable but can be used as the basis for informing future work. An area for further research is to probe if the patterns we observed across beat and professional status hold for journalists from different geographic locations, contexts, and backgrounds, or if differences in culture, economics, politics, and other social factors affect how journalists approach information security. For example, while not systematically analysed in this study our results suggest that gender and medium (e.g., print, video, photojournalism) could be variables that affect how journalists perceive and practice information security. Our study is on the experiences of journalists working in a Western country with a free press system. We expect that the security perceptions and concerns of journalists working in authoritarian states may be significantly different. A focussed study of these variables is needed to understand the potential differences.

As information security threats continue to put source confidentiality and press freedom at risk, journalists and newsrooms need to acknowledge the fluid and fragmented security culture of the profession and make efforts to bridge the gaps.

Disclosure Statement

No potential conflict of interest was reported by the author(s).

Funding

Funding was received from the John D. and Catherine T. MacArthur Foundation.

References

Asgharpour, F., D. Liu, and L. J. Camp. 2007. "Mental Models of Security Risks." In *Financial Cryptography and Data Security*, edited by S. Dietrich, R. Dhamija, 367–377, Berlin, Heidelberg: Springer.

Bennett, W. L. 1990. "Toward a Theory of Press-State Relations in the United States." *Journal of Communication* 40 (2): 103–127.

Canadian Journalists for Free Expression. 2017. "CJFE and press freedom groups condem Ontario court ruling against vice journalist Ben Makuch, 2017." https://www.newswire.ca/news-releases/cjfe-and-press-freedom-groups-condemn-ontario-court-ruling-against-vice-journalist-ben-makuch-616835654.html

CBC. 2016. "6 reporters spied on by Quebec provincial police (2016)." https://www.cbc.ca/news/canada/montreal/quebec-journalists-police-spying-1.3833507

Cohen, N. S. 2016. *Writer's Rights Freelance Journalism in the Digital Age*, Montreal, Quebec, CA: McGill-Queen's University Press.

Das, J. 2007. "Sydney Freelance Journalists and the Notion of Professionalism." *Pacific Journalism Review: Te Koakoa* 13 (1): 142–160.

Drohan, M. 2017. "The Shattered Mirror, public policy forum 2017." https://shatteredmirror.ca/

Edstrom, M., and M. Ladendorf. 2012. "Freelance Journalists as a Flexible Workforce in Media Industries." *Journalism Practice* 6 (5-6): 711–721.

Gollmitzer, M. 2014. "Precariously Employed Watchdogs? Perceptions of Working Conditions among Free- Lancers and Interns." *Journalism Practice* 8 (6): 826–841.

Greenwald, G. 2014. *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State*. New York, NY: Metropolitan Books

Grey, D. L. 1966. "Decision-Making by a Reporter under Deadline Pressure." *Journalism Quarterly* 43 (3): 419–428.

Hanitzsch, T., H. Folker, R. Jyotika, and d. B. Arnold. 2019. *Worlds of Journalism: Journalistic Culture around the Globe*, New York: Columbia University Press

Henrichsen, J. R. 2020. "Breaking Through the Ambivalence: Journalistic Responses to Information Security Technologies." *Digital Journalism* 8 (3): 328–346.

Henrichsen, J. R., M. Betz, and J. M. Lisosky. 2015. *Building Digital Safety for Journalism: A Survey of Selected Issues*, Paris: UNESCO Publishing. http://unesdoc.unesco.org/images/0023/002323/232358e.pdf

Herzog, C., C. Handke, and E. Hitters. 2019. "Analyzing Talk and Text II: Thematic Analysis." In *The Palgrave Handbook of Methods for Media Policy Research*, edited by H. Van, M. Puppis, K. Donders, L. V. Audenhove, 385–401, Cham, Switzerland: Palgrave Macmillan.

Hu, Q., T. Dinev, P. Hart, and D. Cooke. 2012. "Managing Employee Compliance with Information Security Policies: The Critical Role of Top Management and Organizational Culture." *Decision Sciences* 43 (4): 615–660.

Karlsson, F., J. Astrom, and M. Karlsson. 2015. "Information Security Culture State of the Art Review between 2000 and 2013." *Information and Computer Security* 23 (3): 246–285.

Ladendorf, M. 2013. "Freelance Journalists' Ethical Boundary Settings in Information Work." *Nordicom Review* 33 (1): 83–98.

Lee-Wright, P. 2012. "The Return of Hephaestus: Journalists' Work Recrafted." In *Changing Journalism*, by Peter Lee-Wright, Angela Phillips and Tamara Witschge, pp. 21–40. London: Routledge

Mahoney, R. 2015. "Going it alone: More freelancers means less support, greater danger." https://cpj.org/2015/04/attacks-on-the-press-more-freelancers-less-support-greater-danger.php

Mathisen, B. R. 2017. "Entrepreneurs and Idealists." *Journalism Practice* 11 (7): 909–924.

McGregor, S. E., and E. A. Watkins. 2016. "Security by Obscurity: Journalists' Mental Models of Information Security." *Journal of the International Symposium of Online Journalism* 6 (1): 33. https://isojjournal.wordpress.com/2016/04/14/security-by-obscurity-journalists-mental-models-of-information-security/.

McGregor, S. E. F., Roesner, and K. Caine. 2016. "Individual versus Organizational Computer Security and Privacy Concerns in Journalism." In Proceedings on Privacy Enhancing Technologies, PeTs.

McGregor, S. E., P. Charters, T. Holliday, and F. Roesner. 2015. "Investigating the computer security practices and needs of journalists." USENIX Security Symposium. https://www.usenix.org/system/files/conference/usenixsecurity15/sec15-paper-mcgregor.pdf.

Morgan, G., B. Fischhoff, A. Bostrom, and C. Atman. 2001. *Risk Communication*. Cambridge, UK: Cambridge University Press.

Nies, G., and R. Pedersini. 2003. "European Federation of Journalists: freelance journalists in the European media industry report." European Federation of Journalists 2003. https://european-journalists.org/policy/freelance/

OSCE, and W. Horsley, 2014. *Safety of Journalists Guidebook*, 2nd ed. Vienna, Austria: Organization for Security and Co- operation in Europe

Perlroth, N. 2013. "Hackers in China Attacked The Times for Last 4 Months." *New York Times*, January 2013. http://www.nytimes.com/2013/01/31/technology/chinese-hackers-infiltrate-new-york-times-computers.html?{_}r=0

Pew Research Center. 2015. "Investigative journalists and digital security: perceptions of vulnerability and changes in behavior." 5 February, 2015. Pew Research Centre: Journalism & Media. http://www.journalism.org/2015/02/05/investigative-journalists-and-digital-security/

Posetti, J. 2017. *Protecting Journalism Sources in the Digital Age*. UNESCO Series on Internet Freedom. Paris, France: UNESCO. https://unesdoc.unesco.org/ark:/48223/pf0000248054

Professional Writers Association of Canada (PWAC). 2006. *Canadian Professional Writers Survey: A Profile of the Freelance Writing Sector 2006*. Toronto: Quantum. http://pwac.ca/wp-content/uploads/2014/03/PWACsurvey.pdf

Ramachandran, S., C. Rao, T. A. Goles, R. Sanchez, G. Dhillon, and V. Srinivasan Rao. 2013. "Variations in Information Security Cultures across Professions: A Qualitative Study." *Communications of the Association for Information Systems* 33 (11): 163–204.

Ramachandran, S., S. V. Rao, and T. Goles. 2008. "Information Security Cultures of Four Professions: A Comparative Study." Proceedings of the Annual Hawaii International Conference on System Sciences.

Reporters Without Borders. 2017. Canada, 2017. https://rsf.org/en/canada

Ryfe, D. M. 2009. "Broader and Deeper: A Study of Newsroom Culture in a Time of Change." *Journalism: Theory, Practice & Criticism* 10 (2): 197–216.

Schiller, D. 1979. "An Historical Approach to Objectivity and Professionalism in American News Reporting." *Journal of Communication* 29 (4): 46–57.

Schudson, M. 1989. "The Sociology of News Production." *Media, Culture & Society* 11 (3): 263–282.

Schulz, D. A., and V. Belair-Gagnon. 2018. "Rescuing a Reporter's Right to Protect the Confidentiality of Sources." In *Journalism after Snowden*, edited by E. Bell and T. Owen, 97–113, New York: Columbia University Press.

Scott-Railton, J., B. Marczak, B. AdbulRazzak, M. Crete-Nishihata, and R. Deibert. 2017. "Reckless exploit: Mexican journalists, lawyers, and a child targeted with NSO spyware." Citizen Lab, University of Toronto. https://citizenlab.ca/2017/06/reckless-exploit-mexico-nso/

Shelton, M. L. 2015. "The Role of Corporate and Government Surveillance in Shifting Journalistic Information Security Practices." Ph.D. thesis, University of California, Irvine. https://mshelt.onl/p/shelton{_}2015.pdf

Standing Committee on Canadian Heritage. 2017. "Disruption: change and churning in Canada's media landscape." House of Commons Canada 2017. https://www.ourcommons.ca/DocumentViewer/en/42-1/CHPC/report-6

Standing Senate Committee on Transport and Communications. 2006. "Final report on the Canadian news media." House of Commons Canada 2006. https://sencanada.ca/content/sen/committee/391/tran/rep/repfinjun06vol1-e.htm

Thomson, K.-L., R. von Solms, and L. Louw. 2006. "Cultivating an Organizational Information Security Culture." *Computer Fraud & Security* 2006 (10): 7–11.

Timberg, C. 2013. "Hackers break into Washington Post servers." *Washington Post*, Dec 2013. https://www.washingtonpost.com/business/technology/hackers-break-into-washington-post-servers/2013/12/18/dff8c362-682c-11e3-8b5b-a77187b716a3{_}story.html

Tsui, L. 2019. "The Importance of Digital Security to Securing Press Freedom." *Journalism* 20 (1): 80–82.

Van Niekerk, J. F., and R. Von Solms. 2010. "Information Security Culture: A Management Perspective." *Computers & Security* 29 (4): 476–486.

Wagstaff, J. 2014. "Journalists, media under attack from hackers: Google researchers." March 2014. http://www.reuters.com/article/us-media-cybercrime-idUSBREA2R0EU20140328

Walters, E., C. Warren, and M. Dobbie. 2006. *The Changing Nature of Work: A Global Survey and Case Study of Atypical Work in the Media Industry*. Switzerland: The International Federation of Journalists. https://www.ifj.org/fileadmin/images/General_Reports_-_moved_from_old_wesbite/The_Changing_Nature_of_Work__A_Global_Survey_and_Case_Study_of_Atypical_Work_in_the_Media_Industry_April_2006.pdf

Watkins, E. A., M. N. Al-Ameen, F. Roesner, K. Caine, and S. McGregor. 2017. "Creative and Set in Their Ways: Challenges of Security Sensemaking in Newsrooms." USENIX Workshop on Free and Open Communications on the Internet. https://www.usenix.org/system/files/conference/foci17/foci17-paper-watkins.pdf.

Winseck, D. 2016. "Media and internet concentration in Canada report 1984–2015." Canadian Media Concentration Research Project. http://www.cmcrp.org/media-and-internet-concentration-in-canada-report-1984-2015/

Worlds of Journalism. 2016. "Worlds of Journalism: aggregated data on key variables." https://www.worldsofjournalism.org/research/2012-2016-study/data-and-key-tables/

Appendix 1. Interview Guide

Demographics

- How do you describe your professional status (newsroom, freelance, etc.)?
- What media organisations do you work for?
- What mediums have you worked in (print, radio, TV, online)?
- What mediums do you currently work in (print, radio, TV, online)? If more than one, please rank in order of frequency.
- How many years have you been working as a journalist?
- What is your educational background?
- Do you have formal education in Journalism? If so at what level (e.g., Undergraduate, Graduate, Apprenticeship)
- Have you ever received training in physical security?
- Have you ever received training in digital security?

Beat

- What topics do you generally cover?
- Do you consider any of your reporting areas to be sensitive?

Role in Story Creation

- What is your role in creating or producing a story or article?
- Walk me through the development of a typical news story you work on. How do you get from the start of things to publication?
- What are the steps and process?
- What technologies do you use?
- Please think about a specific story that you have published in the last year or so, for which you spoke with a source. (There is no need to tell us the specific story or source, unless you would like to share it.)
- How does this story compare to your typical source interactions?

Sources and Information

- What kinds of sources do you get your information from?
- Why are these sources important for your work?
- What is involved in finding these sources or them finding you?
- Do you do anything special to communicate with sources; do your procedures evervary or change? If so, then how?
- How do you store information provided to you by sources?
- How do you disseminate/communicate information shared by sources?
- Do you have any challenges obtaining information/locating sources?
- How do you overcome these challenges?

Use of Technology

- What kinds of devices do you use for reporting (e.g., mobile phone, laptop, etc.)?
- Who administers/owns these devices?
- Are there multiple users on these devices/accounts?
- Do you use personal devices/accounts for your reporting?
- What technologies do you use for communication (*e.g.*, email, chat, etc.)?
- What technologies do you use to take notes? For recording interviews with sources?
- How do you store your notes/interview recordings?
- Does your workplace have policies on administration and use of devices/software?
- Do you perceive different tools, or operating systems, on internet communications methods are more or less secure?
- Has the process and tools you use for reporting changed since you became a journalist?

Perceptions and Experience with Security Threats

- Have you ever experienced security threats due to your reporting?
- Have you taken security precautions with how you work, based on past experiences you've experienced, or that your colleagues have recounted to you?
- Have you changed your work behaviour in response to possible security risks you have experienced, or become aware of?
- Do you suspect you are under any kinds of danger due to your journalistic work? If so, what do you do to mitigate such danger(s)?

Training/Organisational Policy

- Have you received, or implemented, practices to improve your source/data security?
- Have you receiving any training for digital security in particular?
- Is digital security a high priority for you, or does it compete with other things that are more important (e.g., getting a story out quickly or accurately?)
- Do you think that you have any challenges in how you securing yourself from digital threats? Probe this question on organisational and personal level
- Does your organisation have any formal policies concerning computer security?
- What support/capacities do you need for digital security that you don't currently have?

Appendix 2. Coding Sample

Theme	Code	Description	Data Sample
Values and Mental Models	Sensitivity	Perceptions of sensitivity in regard to sources, story, or other aspects of journalistic work.	*"I definitely sometimes do sensitive stories where I am talking to unnamed sources"*
Perceptions of Threat	Threat: Type	The type of threat categorised as legal, technical, physical, or other).	*"I know for a fact that the government has tried to figure out who one of my sources is … from a legal angle"*
Perceptions of Threat	Threat: Experience	If the threat was directly experienced by participants (or a colleague), or was perceived as a possible risk.	*"We recently had an incident here where someone was emailing and texting threats to the newsroom because we had refused to take down a story that named them when they were involved in a criminal matter"*
Perceptions of Threat	Threat: Target	The target of the threat (e.g., organisation, individual journalist, source).	*"I had a journalistic partner who, found a surveillance van outside his home doing who the hell knows what."*
Perceptions of Threat	Threat: Adversary	The adversary that was involved or suspected to be involved (e.g., law enforcement, companies, individuals, etc.)	*"There's been telecom companies that have threatened[libelcharges] … They threatened to sue."*
Security Practices	Staff: Capacities	Capacities and advantages of being a staff reporter regarding information security	*"the pro [of being on staff] is that you obviously have a … security team … .that is responsible for managing that in-formation and those systems."*
Security Practices	Staff: Constraints	Constraints and disadvantages of being a staff reporter regarding information security	*"I have a large bureaucratic organisation that doesn't prioritise [information security] yet."*

(*continued*)

Continued.

Theme	Code	Description	Data Sample
Security Practices	Freelance: Capacities	Capacities and advantages of being a freelance reporter regarding information security	*Being freelance, means if [authorities] show up, I can prefer to go to jail than hand over any information."*
Security Practices	Freelance: Constraints	Constraints and disadvantages of being a freelance reporter regarding information security	*"You don't necessarily have the same legal protection either way when you're a freelancer"*