How journalists understand the threats and opportunities of new technologies: A study of security mind-sets and its implications for press freedom

Lokman Tsui and Francis Lee
The Chinese University of Hong Kong, Hong Kong

Abstract
This is a study on digital security and press freedom, specifically the freedom from surveillance and the freedom to private and secure communication. We study journalists’ understanding and awareness of digital security practices: their perception of risks and threats of surveillance, and also their awareness of tools and techniques to communicate securely. Based on an empirical study of journalists in Hong Kong, including those who regularly travel to China for work, we build out a theoretical framework for understanding digital security mind-sets of journalists. We found differences in journalists’ behavior depending on how novice or advanced their understanding of digital security are. Journalists with a novice security mind-set will take different actions that produce different outcomes and behavior than those with an advanced security mind-set. We argue that journalists with an advanced security mind-set are able to work on a larger and wider range of (sensitive) stories, suggesting they enjoy a higher degree of press freedom.

Keywords
China, digital security, Hong Kong, mental model, press freedom, security mind-set, surveillance

Introduction
State agencies are massively expanding their capacity for surveillance in the wake of new technologies (Bell and Owen, 2017; Edgar, 2017; Greenwald, 2014). While state
surveillance is not new, what is different from the past is the commercial incentive to collect user data and track user behavior (Zuboff, 2015). However, new technologies not only allow for commercial and state surveillance but also offer renewed opportunities for users to protect themselves against surveillance, such as encryption, raising questions about journalists’ awareness and knowledge to use these tools to privately and securely communicate with sources, colleagues, and editors.

To understand the relationship between surveillance and press freedom, we distinguish between the freedom from surveillance and the freedom to private and secure communication: whereas the freedom from surveillance emphasizes the absence of surveillance, the freedom to private and secure communication instead emphasizes the capacity of a user to communicate privately and securely, even in the presence of surveillance. To understand press freedom in the digital age, it is therefore critical to examine to what extent journalists are aware of and able to use digital security tools.

What kind of mind-sets do journalists have when it comes to digital security? How do journalists not only perceive surveillance risks and threats but also how aware are they of digital security solutions? This article studies digital security mind-sets and practices of journalists based in Hong Kong, including those who travel to and work in China. Many Hong Kong journalists need to work regularly in China to cover news about the mainland. Therefore, depending on their beat and topical focus, journalists in Hong Kong face working conditions ranging from a relatively free reporting environment (Hong Kong) to an environment where journalists face a wide range of threats, including surveillance, physical harassment, or even the threats of arrests (China). Examining Hong Kong journalists thus allows us to see how different reporting environments shape journalists’ thinking and behavior when it comes to digital security.

Theoretically, this article contributes to the broader literature on digital security and press freedom by building a theoretical framework of security mind-sets for journalists that could be applied in other contexts. We argue that understanding the security mind-sets of journalists is important if we want to understand press freedom in the contemporary world: the more aware journalists are of opportunities afforded by new technologies to protect themselves from surveillance, the wider the range and types of stories they can work on, leading to a more free, robust, and vigorous journalistic field.

**Literature review**

**Digital security and press freedom**

Freedom from surveillance is an important and critical part of press freedom. If journalists are to do some of their best work in keeping powerful institutional actors accountable, they need to be able to do so free from the surveillance by these powerful institutional actors. The research on press freedom so far mostly is concerned with the legal and physical dimensions of surveillance, but pays less attention, if any at all, to the threat of digital surveillance (see, for example, Becker et al., 2007; Bezanson, 2010; Bollinger, 2010; Carlsson and Poyhtari, 2017; Ruby et al., 2016; The Hong Kong Journalists Association, 2017). That is unfortunate, because the renewed capacities of the surveillance state in a digital age (Edgar, 2017; Granick, 2017; Greenwald, 2014; Zuboff, 2015)
raise important questions for press freedom. Rusbridger (2017), the former editor-in-chief of *The Guardian*, argues that any journalist with even a cursory understanding of the Snowden revelations should understand digital security:

> [S]tates – even liberal democracies – have the ability to intercept, store, and analyze virtually all forms of electronic communication. Faceless people in shadowy agencies (not to mention the police) can, if they wish, read your text messages and e-mails. They can see who or what you’ve been searching for. They can divine what you’re thinking. They can access all your contacts. And they can follow you. (p. 21)

As Rusbridger argues, it is critical for journalists to understand digital security in order to be able to do their work in a way that is free from surveillance. But while Rusbridger makes a compelling argument, many questions remain open and in need to be empirically studied. For example, how do journalists understand digital security and surveillance, how do they perceive risks and threats, are they aware of tools that can help them protect against surveillance, and can they ultimately maintain secure and private communications with their colleagues, editors, and sources, including whistleblowers (Lashmar, 2017; Waters, 2017)?

Yet, digital security can be really challenging and difficult to properly put in practice. Many scholars have tried to understand what factors shape or influence users’ digital security behavior (Abu-Salma et al., 2017; Fagan and Khan, 2016), including the stories or folk models they hear (Rader et al., 2012; Wash, 2010); economic, psychological, or sociological explanations (Anderson, 2001; Odlyzko, 2003); issues of usability, user experience, and user interface of software (Whitten and Tygar, 1999); and user perceptions on whether security practices matter at all or whether they are ultimately futile (Kang et al., 2015). One promising angle is the study of users’ mental models or mind-sets and how they explain security behavior (Asgharpour et al., 2007; Bravo-Lillo et al., 2011; Camp, 2009; Dutton, 2017). A mental model can be defined as ‘an internal conception for how something works in the real world’ (Asgharpour et al., 2007), while a mind-set can be understood as a framework that is relatively firm and used to think about matters of significance (Dutton, 2017). For the purpose of this article, we use the terms ‘mental model’ and ‘mind-set’ interchangeably, although we recognize there are subtle differences; a mind-set points to a matter of general attitude and orientation, whereas the phrase mental model connotes something a bit more elaborate and systematic.

Research suggests mental models or mind-sets can be helpful in understanding digital security behavior. For example, Bravo-Lillo et al. (2011) argue that there are significant differences between the mental models of novice and advanced users, and that correspondingly, they perceive risks and warnings differently, therefore arrive at different diagnoses and ultimately respond in different ways. In addition, Chin et al. (2012) argued that it is important to understand the level of confidence users have in their own understanding of security issues, because it is possible users, especially novice users, can have misperceptions about security.

While there are many studies focused on explaining users’ security behavior, there are far fewer studies specifically focusing on journalists’ security behavior. Digital security studies of journalists have been done in Pakistan (Internews, 2012), Mexico (Freedom
House, 2013), and the United States (Pew Research Center, 2015; Tow Center for Digital Journalism, 2015). While these studies are valuable, they are ultimately more descriptive in nature and lack a theoretical framework that might explain the security behavior of journalists. An important exception is a McGregor and Watkins (2016) study, which uses the mental model as a theoretical framework to understand digital security practices of journalists. They found that the way most journalists think about digital security can best be described as ‘security by obscurity’: security only matters if they need to handle sensitive materials, but in most daily and mundane journalistic work, digital security is not something that they consider necessary. The study is based on interviews with 15 journalists and 7 editors, primarily from the United States with some based in Europe, working for both small and large news organizations. However, it remains an open question what mental models journalists in other places besides the United States and Europe rely on for understanding digital security. The mental model as a nascent theoretical framework for understanding security behavior of journalists is promising but needs additional empirical research and further theoretical analysis. As argued, the Hong Kong context makes particular sense for studying this question. Hong Kong has a tenuous relationship with press freedom, one where press freedom is deteriorating. But at the same time, there are also legal and physical limitations to how Beijing can control the media. Journalists based in Hong Kong often travel back and forth and experience different levels of surveillance and press freedom, and therefore constitute a strategic case for understanding the larger questions about digital security and press freedom.

**The critical case of Hong Kong**

The dominant narrative about the decline of press freedom in Hong Kong pinpoints the political economy of the city’s media system as the root of the problem. Under ‘One Country, Two Systems’, the Chinese state cannot exercise direct control of the Hong Kong press. What it has done since the early 1990s is to co-opt the major media owners in Hong Kong, most of whom are tycoons with vast business interests in the mainland (Lai, 2007). Many of these media owners also have political titles in China, such as being members of the Chinese People’s Political Consultative Committee (Ma, 2007). Although the owners may not intervene in the daily operations of news organizations, they make decisions regarding the key personnel of the news organizations and set the basic parameters of resource allocation. Control and influence can then filter down to the newsroom hierarchies, and the result is widespread practice of self-censorship (Cheung, 2010; Lee, 1998, 2015; Lee and Chan, 2006; Lee and Lin, 2009; The Hong Kong Journalists Association, 2017). Without disputing the main thrust of the above dominant narrative, we believe that digital security is an important additional dimension to the question of press freedom that needs to be taken into account. Hong Kong journalists generally acknowledge the significant impact of the Internet on journalistic work. In a representative survey of Hong Kong journalists conducted in 2011, 94.2 percent of the respondents agreed that ‘the Internet can enhance the efficiency of news work’, whereas 86.6 percent agreed that ‘the Internet has very large contribution to news work overall speaking’. While the importance of the Internet for journalists in Hong Kong is growing, at the same time concern for surveillance is also growing, especially among activists,
legislators, and journalists (Hargreaves, 2017; Tsui, 2015). Beijing has a long and extensive record of conducting surveillance and censorship on the mainland: the Great Firewall is not only a censorship or filtering technology but also a surveillance infrastructure (Tsui, 2003; Walton, 2001). Surveillance is often outsourced to companies. For example, in 2008, it was revealed that Tom-Skype, the Chinese version of the popular chat program Skype, would track what users were communicating with each other and it would report on the conversation every time a sensitive keyword was detected (Villeneuve, 2008). In addition, there is extensive evidence of civil society groups and journalists being targets of cyber espionage, especially those that are of political interest to the Chinese government (Lab, 2009). Moreover, there is evidence of China-based operators conducting network intrusions into news organizations, including *The New York Times*, *The Washington Post*, *The Wall Street Journal*, and *Bloomberg*, leading *The New York Times* to ask: ‘The question is no longer who has been hacked. It’s who hasn’t?’ (Perlroth, 2013). In addition to Beijing, the local Hong Kong government has also expressed interest in digital surveillance: the Independent Commission Against Corruption (ICAC) made inquiries to Hacking Team, an Italian company notorious for selling surveillance software and services to governments, including those with poor human rights records, that would allow them to take over, control and spy on people’s smartphones and computers (Lam, 2015). Last but not least, there are few legal protections against digital surveillance in place: the legislature passed the Interception Communication Surveillance Ordinance (ICSO) in 2006 (Wong, 2008), which details the requirements upon which surveillance of telephone, fax, and postal mail can be conducted by law enforcement. But despite repeated attempts by legislators to seek clarification, the government has refused to confirm whether the ICSO covers digital communication, such as email and chat apps (Legislative Council, 2015). Against this background, there is an imminent need to understand how journalists in Hong Kong understand and practice digital security.

Yet, there are few studies on journalists’ understanding of digital security in Hong Kong. While not directly focused on digital security, one study looks at how foreign correspondents in Hong Kong use chat apps for sourcing purposes (Belair-Gagnon et al., 2018; see also Belair-Gagnon et al., 2017). Similar to the McGregor and Watkins (2016) study, they found that foreign correspondents primarily defer to sources in deciding how to communicate, which often meant using less secure means of communication. Knowing the chat apps are insecure, many journalists rely on a ‘hiding in plain sight’ strategy where they obfuscate messages by using code words or misspell words to avoid scrutiny. While valuable, their study focuses on the usage of chat apps in talking to sources by English-speaking foreign correspondents based at international media organizations that are often better resourced than local media organizations. A study of digital security, however, would need to entail a wider range of activities and services, including understanding how journalists communicate with sources, colleagues, and editors in addition to mobile chat apps, such as encrypted email on desktop or laptop devices, but also how they archive or delete their transcripts and documentation. This article thus contributes to the existing literature by studying the security mind-sets and mental models of journalists at local media organizations in Hong Kong.
Methodology

We conducted semi-structured interviews with 20 journalists in Hong Kong between July 2016 and March 2017. We sent email invitations through our existing relationships within the journalism community in Hong Kong and through referrals we received. We explained we wanted to discuss how new technologies have affected their work, with a particular focus on understanding digital security.

We relied on grounded theory (Glaser and Strauss, 1967) to allow theoretical concepts and findings to surface. A team of four coders went over the transcripts several times for a deep reading and discussed the findings (see Appendix 1 for coding samples). The interview was designed to be open-ended, meaning we did not explicitly ask about digital security, but instead allowed it to surface if the conversation took us there. For example, instead of asking ‘do you use security tools to protect yourself?’, we probed deeper when the topic of sensitive stories and sources came up, asking ‘would you do anything special to communicate with this source?’ We made a conscious effort to listen for the silences in the conversation, given that some participants might not consider themselves to be technically savvy.

Our interview script was organized in five sections: we started by asking what topics they generally cover, what role they play in producing a news story, and whether they could walk us through the production flow of a typical news story. We then asked questions about how they interact with sources, how they find them, how they communicate with them, and if they do anything special to communicate with them. We also asked questions about the use of technology, including what devices they use, what they use to take notes, and how they store their notes. Last but not least, we asked about their perceptions and experience with security threats, including whether they have received any security training or whether their organization has any policies related to digital security. Please refer to Appendix 2 for our interview script.

Most interviews took place in a semi-public space such as a cafe or hotel lounge, while some took place in participants’ offices. All interviews were conducted in Cantonese. We recorded the interviews using a digital voice recorder. We coded participants’ names in the transcripts and translations, and we stored the files on an encrypted hard drive. Two research assistants helped with transcribing and translating the interviews into English. They were given a soft copy of the transcripts and asked to delete the transcripts from their laptop when they were done.

For background information of the participants, please see Table 1. We sampled reporters from a range of media, including print and broadcast news organizations, and news organizations with an exclusive ‘online only’ presence. We oversampled for journalists working in investigative reporting and those who often work in China, given that the literature suggests that perceived sensitivity of the work shapes and influences how journalists practice digital security (McGregor and Watkins, 2016). For similar reasons, we oversampled for journalists working for news organizations considered pro-democratic or critical of Beijing, although we also included a small number of reporters from pro-establishment news organizations. Note that given the lack of ‘online only’ news organizations in Hong Kong (excluding organizations that might qualify as alternative or citizen media), we interviewed only two reporters from an
To get a comprehensive view, we interviewed three senior managers, five journalism educators, as well as a reporter working in financial news and one in photojournalism. We not only interviewed the senior managers and journalism educators in the context of their current role as manager or educator but also asked them to relate their former experience as a journalist to us, giving us a sense of the historical and technological development of security practices over time.

**Ethics**

We received approval from the Ethics Review Board before we conducted the interviews. We explained that we would redact references to their name or their organization in any publication, and that instead we would describe their general professional role and the profile of their organization. We explicitly acknowledged that, depending on the detail of the experiences they would share with us, it might be possible for people in the field to deduce their identities given the relatively small community of journalists in

| Number | Current roles            | Gender | Type of news organization | Interview length | China beat experience | Investigative beat experience |
|--------|--------------------------|--------|---------------------------|------------------|-----------------------|------------------------------|
| 1      | Educator, journalist     | M      | Education, broadcast      | 1:43:49          | Yes                   | No                           |
| 2      | Journalist               | M      | Print                     | 1:47:18          | No                    | Yes                          |
| 3      | Journalist               | M      | Print                     | 1:07:09          | No                    | Yes                          |
| 4      | Journalist               | M      | Print                     | 1:21:23          | No                    | Yes                          |
| 5      | Journalist               | M      | Print                     | 1:05:20          | No                    | Yes                          |
| 6      | Photojournalist          | M      | Print                     | 1:47:18          | No                    | No                           |
| 7      | Journalist               | M      | Broadcast                 | 1:26:04          | No                    | No                           |
| 8      | Journalist               | M      | Broadcast                 | 1:16:16          | No                    | No                           |
| 9      | Journalist               | W      | Online                    | 1:26:15          | No                    | No                           |
| 10     | Manager, educator        | M      | Broadcast, education      | 1:26:43          | Yes                   | No                           |
| 11     | Journalist               | M      | Print                     | 2:08:31          | No                    | Yes                          |
| 12     | Journalist               | W      | Print                     | 1:37:00          | No                    | No                           |
| 13     | Manager                  | M      | Broadcast                 | 00:45:58         | N/A                   | N/A                          |
| 14     | Manager                  | W      | Broadcast                 | 1:49:49          | N/A                   | N/A                          |
| 15     | Journalist               | W      | Online                    | 1:52:54          | No                    | No                           |
| 16     | Journalist               | M      | Broadcast                 | 2:21:09          | Yes                   | No                           |
| 17     | Educator                 | M      | Education, broadcast      | 1:09:11          | Yes                   | No                           |
| 18     | Educator, journalist     | W      | Education, print          | 1:02:03          | No                    | Yes                          |
| 19     | Educator, journalist     | W      | Education, broadcast      | 1:23:30          | No                    | No                           |
| 20     | Journalist               | W      | Print                     | 1:16:52          | Yes                   | No                           |
We also explained that they could refuse to answer a question, request part of an answer to be off-record, or even stop the interview if they felt uncomfortable.

**Findings**

From our interviews, we found groups with different security mind-sets emerging, some more developed than others. Among the 20 participants, 10 had a novice ‘security by obscurity’ mind-set, 7 fell into the ‘security by obfuscation’ category while 3 had the advanced ‘security as opportunity’ mind-set.

From our interviews, a picture of a security mind-set emerged consisting of two components: threat awareness and protection awareness. Related to the freedom from surveillance, threat awareness constitutes knowledge of potential threats facing journalistic work. Related to the freedom to secure and private communication, protection awareness entails knowledge of tools, technologies, or techniques that can be used for protection against surveillance. All journalists we talked to had some awareness of threats, whether legal, physical, or digital, but some were much more comfortable talking about threats in detail and specificity than others. For example, journalists with a low threat awareness would attribute vague and often almost omnipotent powers to the state apparatus, whereas journalists with a high threat awareness would have a reasonable understanding for how state surveillance works, including a willingness to examine how its mechanisms might change over time.

However, it was when we started analyzing protection awareness that an even more significant difference between journalists with a novice versus an advanced security mind-set became clear. Journalists with a low protection awareness did not know much about the various digital security tools and techniques. They would often rely on low-tech means for protection, including using code words to mitigate the threat of surveillance, or meeting in person instead of having a conversation online. In contrast, journalists with a high protection awareness were comfortable with a wider range of techniques, both low-tech and high-tech. Examples of the latter include encrypted chat apps or Virtual Private Networks (VPNs). Our typology and theoretical model does not assume that high-tech techniques are better than low-tech ones, but that being able to command both high-tech and low-tech techniques is preferable over being able to only use low-tech. Broadly speaking, the higher the protection awareness, the wider the range, the larger the number, and the more complex and sophisticated the techniques are that they can employ to protect themselves.

Following the dimensions of threat awareness and protection awareness, we build on the existing security mind-set (‘security by obscurity’) found by McGregor and Watkins

| Model    | Threat awareness | Protection awareness |
|----------|------------------|----------------------|
| Obscurity| Low              | Low                  |
| Obfuscation | High            | Low                  |
| Opportunity | High             | High                 |
Tsui and Lee (2016) and propose two additional security mind-sets, ‘security by obfuscation’ and ‘security as opportunity’. Please refer to Table 2 for a typology of the different security mind-sets.

**Security by obscurity**

The first group follows the ‘security by obscurity’ model (McGregor and Watkins, 2016) and has a novice security mind-set. The notion of obscurity here refers to the journalists’ belief that digital security is not necessary, because their work is not sensitive or important enough. Another way to look at this is that they ‘protect’ themselves by working on non-sensitive news stories. They often believe that the primary threats are not digital but rather legal in nature. They thus emphasize the need to protect themselves against being sued for defamation or libel, but have an incomplete mental model of digital threats. They do not deny that the government might practice surveillance or target journalists, but they do not see it interfering with their work. Some also might believe there is nothing that can be done about it, that if ‘they’ really want to know what you are doing, ‘they’ will find out. A senior manager from a broadcast news organization put it like this:

> But there is not much sensitive issue in Hong Kong, we don’t need to be too nervous when we are dealing with the source.

In another example, one manager with a novice security mind-set preached that journalistic integrity was the most important form of protection, arguing that as long as a journalist is professional, has heart, and reports the news in an accurate manner, that is what matters and that is what is important. When asked about the possibility of email being hacked or being the target of surveillance, she answered,

> I have no such experience before. I don’t think I have any secrets. Therefore I’m not a target for hacking. I haven’t got worried about it before.

Relatedly, managers often displayed a ‘security by obscurity’ mind-set, arguing there was little to fear in Hong Kong because ‘there is no big issue in Hong Kong, I don’t think there is any’.

‘Security by obscurity’ is primarily (but not exclusively) practiced by journalists based in Hong Kong who operate in Hong Kong. This group includes both investigative and non-investigative reporters; whether one does investigative reporting in Hong Kong or not does not seem to necessarily correlate with concern for digital threats, including government surveillance. If they do take any precautions, it is to archive their documents, but this is in large part because of organizational policy rather than individual initiative.

**Security by obfuscation**

The second group is ‘security by obfuscation’ and also has a relatively novice security mind-set. The notion of obfuscation refers to the journalists’ belief that they can protect themselves
by obfuscating their digital communication through the use of low-tech techniques, such as by speaking in code words or misspelling words. We found participants with the ‘security by obfuscation’ mind-set in both the group of reporters working in Hong Kong and those who cover China. For those in Hong Kong, security by obfuscation primarily meant resorting to meeting in person with sources and not communicating electronically to minimize the potential exposure to surveillance. To some extent, this practice makes sense, given the geography and small size of Hong Kong and thus the relative ease, affordability, and convenience to meet in person.

For journalists working in China, a dominant and recurring theme for participants was the risks and challenges of having to use WeChat, an app that is insecure and subject to surveillance, but is also the most popular messaging app in China that offers services such as one-on-one chat, group chat, payments, games, and social networking. WeChat is an insecure app because none of the communication on WeChat is end-to-end encrypted, meaning that discussions on WeChat can be monitored by the company itself and state agencies. WeChat users in China are subject to censorship and individuals have been arrested or detained based on content they shared on the platform (Dou, 2017; Ruan et al., 2016). The ‘security by obfuscation’ group deals with this challenge primarily by relying on low-tech techniques, explaining that they would not discuss anything meaningful over WeChat but instead would wait until they met in person.

Finally, a last resort mentioned by both journalists and senior managers is to withdraw entirely from a story, because sometimes the risk of a specific sensitive story is too large and even a minimum level of security cannot be guaranteed. Some of our interviewees who are veterans in China news reporting noted that they relied on their own experience as well as insider information from stringers to judge when a story had become too dangerous to work on. One reporter from a print-based organization said,

I don’t worry about the Public Security people … if you get attention from Public Security, it only means you are unable to cover that story. Only recently they do start to beat you up, but that’s something else. They are only trying to stop you from working. However, if they are not from Public Security, what will happen? It’s local power. Once I went to Hebei Province, I don’t remember what for, when I entered some places, there was no Public Security people, but some other people were waiting for you. Who were they? Local power. That dark power is connected to the local government. Therefore we dare not work there. […] You can go there anytime you want, but you dare not do so. When you enter the village, you get killed before you know what is going on. When you are in Beijing, Shanghai, you can do that, because you are in broad daylight, relatively in broad daylight. So those stories are untouchable, those cases that are related to your own safety.

However, in some cases, it is possible that knowing how to use the right tools for security would enable and empower reporters to do stories that they otherwise would not be able to work on. This brings us to the discussion of ‘the security as opportunity’ group.

Security as opportunity

The ‘security as opportunity’ group is characterized by journalists with an advanced security mind-set. ‘Opportunity’ here refers to the journalists’ belief that security does
not only have to be a business cost but can also be a business opportunity, allowing them to work on stories they otherwise might not be able to do. It is why they continue to educate themselves on digital security threats and protections, and learn to master new tools and techniques. They can thus work on a larger number of stories and are not as limited as the other journalists in the type of stories they can work on. In comparison, the ‘security by obscurity’ group can only work on stories that they consider not sensitive, whereas the ‘security by obfuscation’ group can work on sensitive stories but only to the extent that low-tech techniques can protect them. To put it in economic terms, ‘obscurity’ does not consider digital security a necessary business cost, unless you work on sensitive stories; ‘obfuscation’ considers security to be a necessary cost of doing business; and ‘opportunity’ considers digital security an opportunity. See Table 3 for how groups with different security mind-sets view digital security differently in terms of cost and opportunity.

The ‘security as opportunity’ group was comfortable discussing high-tech techniques such as the use of encrypted chat apps and VPNs to circumvent censorship and to preserve a level of privacy. But it would be an incomplete picture to say that they distinguished themselves merely by knowledge or familiarity of tools. Rather, an even more important distinction is the willingness to learn and to see these tools as opportunities for even better protection and for doing better journalistic work. As one senior reporter from a print-based media said,

I think it is an attitude, not a skill. The attitude is to do your job well. That’s why I think it is a matter of awareness. They need to find a way to ensure safety … and be able to do your job at the same time. How would you try all means to accomplish this goal?

We asked the participants with the ‘security as opportunity’ mind-set what made them different. Why do they practice digital security while many of their colleagues do not? Many mentioned that this was a simple question of journalism ethics, that it is their duty to protect their sources. Practicing digital security also had a strategic aspect: they saw going out of their way to protect their sources as potentially beneficial for their reputation. Last but not least, they often pushed back on our question, arguing that we instead should be asking why the others do not practice or learn digital security. They do not see security as an additional or optional burden, but instead as a kind of responsibility and a necessary cost of doing business. Dutton (2017) compares this with buying a bike: whether to buy a lock or not is for most people in most places not an option; a bike lock is simply a necessary cost if you want to use the bike and you do not want it to get stolen. Our participants similarly argued, if you want to practice journalism in China, learning

Table 3. Perception of digital security.

| Security mind-set | Perception of digital security |
|-------------------|--------------------------------|
| Obscurity         | Not a necessary business cost  |
| Obfuscation       | A necessary business cost      |
| Opportunity       | A business opportunity         |


about and practicing digital security is not an option, it is just necessary. But they also realize that this comes down to awareness. They saw digital security as something they should be doing but realize this is not the norm. In one participant’s words,

You shouldn’t think ‘it is okay that my files are read’. You can’t have this kind of attitude. Awareness is what matters the most. Some people might think that the authorities are omnipotent, they can read anything they want. I can’t avoid them regardless of what app I use. Some people really think like that. I believe how they think matter more than what skill or app they use.

In contrast to other participants, the ‘security as opportunity’ group was much less inclined to see the authorities as omnipotent. They also distinguished between different state authorities, instead of conflating them all, demonstrating a situational understanding of their adversaries and threat models. One participant mentioned a conversation she had with her boss:

Sometimes the boss would joke ‘even if the Chinese government does not read [our messages], the American government does. You think they don’t read your Gmail?’ I would respond ‘yes, but I’d rather they were read by the American government. Or my Kakao were being watched by the Korean government. I just don’t want them to be read by the Chinese government’.

The different levels of awareness between those with a novice and those with an advanced security mind-set often created problems for collaboration in the newsroom and sometimes even gave rise to conflict. One participant stated this as follows:

That’s why we have to go and convince everyone to do so. Because in addition to communicating with interviewees, the most important communication is between us and our organization. Everything we have we’ll need to send back to the office. I think whether the organization decides to adopt the technology is very important. It is very difficult to talk everyone into installing a certain app.

One participant not only tried to convince her colleagues to use a more secure chat app, she tried to get rid completely of email and phone as means of communication:

We try our best to avoid phone calls and emails. It’s much better, thanks to 3G, 4G … We used to use Gmail but since it was heavily cracked down, we’ve switched to instant messaging systems. We don’t have to use emails now. We actually explored many options to avoid using emails.

Journalists with different security mind-sets perceived the Information Technology (IT) department in their news organization in different ways. The journalists with a novice security mind-set often worked with the IT department and followed their instructions. In contrast, the journalists with an advanced security mind-set often had conflicts with the IT department and found them not to be very helpful and sometimes even saw them as hostile. One participant, for example, told us:
In my opinion, on one thing, it [the IT department] would not set up a VPN for China reporting team. Some news organizations have it but we don’t. Yes, they then set up one, but it didn’t work that well. I ended up buying another VPN just in case.

Another participant made light of the situation:

We use our own way. We don’t trust the company’s IT department! Same thing in every company! [Laugh]

One participant mentioned that at any given time, he had subscriptions to three different VPNs. We asked why he needed so many, and he mentioned that he rotates them based on how useful they are; sometimes one VPN is slower or blocked, and he would then use another. We also asked if he was paying this out of pocket or if he claimed this as a business expense:

The company won’t pay you for these things.

Perhaps even more important than the IT department were the managers. Our findings suggest that the managers were perhaps the least aware or familiar with both threats and protection. One journalist with an advanced security mind-set criticized management and attributed their indifference to security to low awareness, arguing it is not an issue of (lack of) resources:

Yes, their awareness is poor. Resources will be provided after an attack, and it’s not costly, therefore I don’t blame on resources. If you ask me, I blame on the poor awareness. Very, very poor sense, a sense as if in the Stone Age.

**Conclusion**

Our research shows that there are critical differences between journalists with a novice and an advanced security mind-set. Those with a more advanced security mind-set (security as opportunity) are more aware of how to protect themselves, allowing them to communicate securely and safely with colleagues and with sources. They also actively seek to educate and empower themselves by continually learning about tools and techniques they can use for protection. Our research shows a close relation between security mind-set and the extent to which reporters can effectively exercise their freedom, that is, the security mind-set of a journalist may limit or broaden the range and type of stories he or she can work on; journalists who actively improve their awareness of digital security can also enlarge the range and type of stories they can work on. We need to understand press freedom as a ‘positive’, not just as a ‘negative’, liberty (Berlin, 1969). That is, not just freedom from surveillance but also the freedom to produce specific types of ‘sensitive’ stories, which require a capability to communicate privately and securely with your colleagues, editors, and sources.

This study has both theoretical implications for our understanding of press freedom, surveillance, and digital security, and practical implications for news organizations and journalists. Surveillance is by design invisible; that is why it is important we continue to
make surveillance visible if we want to understand how surveillance threatens press freedom. Yet, because of its invisible and pervasive nature, we can never be quite sure that there is an absence of surveillance (freedom from surveillance). It is why most of our participants with a novice security mind-set displayed a sense of resignation, suggesting that nothing is ever secret or private in today’s age and that the state knows everything anyway if they want to. In contrast, a small number of participants with an advanced security mind-set (‘security as opportunity’) had a different attitude and saw digital security as a critical means to advance press freedom. They see digital security as a critical factor to ensure and enjoy the freedom to communicate privately and securely possible.

There seems to be a correlation between security mind-set and location. Our findings suggest that to a large extent, but not exclusively so, the journalists with a more advanced security mind-set were those working on the China beat (see Table 4 for an overview). Those who only worked in Hong Kong or those not actively working on the frontline, such as managers, had a more novice security mind-set. The correlation is not perfect though, as one Hong Kong investigative journalist, who entered the field originally as a spot news journalist, was one of the most security-aware participants in our study. We also acknowledge that our study has been limited to staff journalists at professional news organizations based locally in Hong Kong. More studies in other contexts are necessary, including journalists working in other regions that might be considered sensitive from a press freedom perspective.

Based on our findings, we encourage journalists to pay more attention to the opportunities and benefits offered by digital security. Given the invisible nature of surveillance, all journalists might encounter digital threats at least occasionally. To use the bike analogy, journalists should not wait with learning how to use a lock until they are biking to a ‘sensitive’ area, or after their bike has been stolen. We also encourage news organizations to play a more active role in setting policies that make it easier for journalists to adopt and use digital security tools. Our analysis highlights the role of news organizations in facilitating and sometimes undermining the security mind-set of journalists. For example, no participants mentioned having received any digital security workshop or training through their organizations; any digital security skills and knowledge were learned through interaction with peers or by self-education. To belabor the point, news organizations have an important role to play in actually enhancing the security of the organizations’ systems and encourage journalists to get more acquainted with digital security issues, especially because it is not realistic to expect every journalist to educate themselves on digital security issues or to pay for digital security out of pocket. How individual career trajectories, organizational contexts, and the broader social contexts for

| Security mind-set | Number | China beat | Investigative beat |
|------------------|--------|------------|--------------------|
| Obscurity        | 10     | 0          | 4                  |
| Obfuscation      | 7      | 3          | 1                  |
| Opportunity      | 3      | 2          | 1                  |
journalistic work intersect to shape a journalist’s security behavior can be a topic for future studies to address.

Funding
The author(s) disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: The study was supported by John D. and Catherine T. MacArthur Foundation (SS16771).

ORCID iD
Lokman Tsui https://orcid.org/0000-0002-7608-1690

References
Abu-Salma R, Angela Sasse M, Bonneau J, et al. (2017) Obstacles to the adoption of secure communication tools. In: Proceedings of the 2017 IEEE symposium on security and privacy. Available at: https://www.ieee-security.org/TC/SP2017/papers/84.pdf

Anderson R (2001) Why information security is hard: An economic perspective. In: Proceedings of the 17th annual computer security applications conference, New Orleans, LA, 10–14 December.

Asgharpour F, Liu D and Camp LJ (2007) Mental models of security risks. In: Proceedings of the 11th international conference on financial cryptography and 1st international conference on usable security, Scarborough, ON, Canada, 12–16 February, pp. 367–377. New York: IEEE.

Becker LB, Vlad T and Nusser N (2007) An evaluation of press freedom indicators. The International Communication Gazette 69(1): 5–28.

Belair-Gagnon V, Agur C and Frisch N (2017) The changing physical and social environment of newsgathering: A case study of foreign correspondents using chat apps during unrest. Social Media + Society. Available at: https://journals.sagepub.com/doi/full/10.1177/2056305117701163

Belair-Gagnon V, Agur C and Frisch N (2018) Mobile sourcing: A case study of journalistic norms and usage of chat apps. Mobile Media & Communication 6(1): 53–70.

Bell E and Owen T (eds) (2017) Journalism after Snowden: The Future of the Free Press in the Surveillance State. New York: Columbia University Press.

Berlin I (1969) Four Essays on Liberty. Oxford: Oxford University Press.

Bezanson RP (2010) How Free Can the Press Be? Urbana, IL; Chicago, IL: University of Illinois Press.

Bollinger LC (2010) Uninhibited, Robust, and Wide-Open: A Free Press for a New Century. New York: Oxford University Press.

Bravo-Lillo C, Cranor LF, Downs J, et al. (2011) Bridging the gap in computer security warnings: A mental model approach. IEEE Security & Privacy 9: 18–26.

Camp LJ (2009) Mental models of privacy and security. IEEE Technology and Society Magazine 28: 37–46.

Carlsson U and Poyhtari R (eds) (2017) The Assault on Journalism: Building Knowledge to Protect Freedom of Expression. Goteborg: Nordicom.

Cheung ASY (2010) Self-censorship and the struggle for press freedom in Hong Kong. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1683823

Chin E, Felt AP, Sekar V, et al. (2012) Measuring user confidence in smartphone security and privacy. In: Proceedings of the eighth symposium on usable privacy and security. Article 1, Washington, DC, 11–13 July.
Dou E (2017) Jailed for a text: China’s censors are spying on mobile chat groups. *The Wall Street Journal*. Available at: https://www.wsj.com/articles/jailed-for-a-text-chinas-censors-are-Spying-on-mobile-chat-groups-1512665007

Dutton W (2017) Fostering a cyber security mindset. *Internet Policy Review* 6(1). Available at: https://policyreview.info/articles/analysis/fostering-cyber-security-mindset

Edgar TH (2017) *Beyond Snowden: Privacy, Mass Surveillance, and the Struggle to Reform the NSA*. Washington, DC: Brookings Institution Press.

Fagan M and Khan MMH (2016) Why do they do what they do? A study of what motivates users to (not) follow computer security advice. In: *Proceedings of the twelfth symposium on usable privacy and security*, Denver, CO, 22–24 June, pp. 59–75. Berkeley, CA: USENIX Association.

Freedom House (2013) Digital and mobile security for Mexican journalists and bloggers. Available at: https://freedomhouse.org/sites/default/files/Digital%20and%20Mobile%20Security%20for%20Mexican%20Journalists%20and%20Bloggers.pdf

Glaser BG and Strauss A (1967) *The Discovery of Grounded Theory: Strategies for Qualitative Research*. Piscataway, NJ: Aldine Transaction.

Granick JS (2017) *American Spies: Modern Surveillance, Why You Should Care, and What to Do about It*. Cambridge: Cambridge University Press.

Greenwald G (2014) *No Place to Hide: Edward Snowden, the NSA, and the US Surveillance State*. London: Palgrave Macmillan.

Hargreaves S (2017) Online monitoring of ‘localists’ in Hong Kong: A return to political policing? *Surveillance & Society* 15(3–4): 425–431.

Internews (2012) Digital security and journalists: A snapshot of awareness and practice in Pakistan. Available at: https://reliefweb.int/report/pakistan/digital-security-and-journalists-snapshot-awareness-and-practice-pakistan

Kang R, Dabbish L, Fruchter N, et al. (2015) ‘My data just goes everywhere’: User mental models of the internet and implications for privacy and security. In: *Proceedings of the 2015 symposium on usable privacy and security*, Ottawa, ON, Canada, 22–24 July, pp. 39–52. Berkeley, CA: USENIX Association.

Lab C (2009) Tracking GhostNet: Investigating a cyber espionage network. Available at: https://citizenlab.ca/wp-content/uploads/2017/05/ghostnet.pdf

Lai CP (2007) *Media in Hong Kong: Press Freedom and Political Change, 1967–2005*. London and New York: Routledge.

Lee FLF (2015) Hacked emails show Hong Kong’s ICAC sought encryption-cracking surveillance software. *The South China Morning Post*. Available at: http://www.scmp.com/news/hong-kong/law-crime/article/1839945/hacked-emails-show-hong-kongs-icac-sought-encryption

Lee FLF and Chan J (2009) Organizational production of self-censorship in the Hong Kong media. *The International Journal of Press/Politics* 14(1): 112–133.

Legislative Council (2015) Official record of proceedings. Available at: http://www.legco.gov.hk/yr14-15/english/counmtg/hansard/cm20150429-translate-e.pdf
Ma N (2007) *Political Development in Hong Kong: State, Political Society, and Civil Society*. Hong Kong: Hong Kong University Press.

McGregor SE and Watkins EA (2016) ‘Security by obscurity’: Journalists’ mental models of information security. *ISOJ* 6(1). Available at: https://pdfs.semanticscholar.org/4c90/d1233601bdcdf10ac2925869eca26be04647.pdf

Odylyzko A (2003) Economics, psychology, and sociology of security. *Lecture Notes in Computer Science* 2742: 182–189.

Perlooth N (2013) Washington post joins list of news media hacked by the Chinese. *The New York Times*. Available at: http://www.nytimes.com/2013/02/02/technology/washington-posts-joins-list-of-media-hacked-by-the-chinese.html

Pew Research Center (2015) Investigative journalists and digital security: Perceptions of vulnerability and changes in behavior. Available at: https://www.journalism.org/2015/02/05/investigative-journalists-and-digital-security/

Rader E, Wash R and Brooks B (2012) Stories as informal lessons about security. In: *Symposium on usable privacy and security*. Washington, DC, 11–13 July, pp. 1–17. New York: ACM.

Ruan L, Knockel J, Ng JQ, et al. (2016) One App, two systems: How WeChat uses one censorship policy in China and another internationally. Available at: https://citizenlab.ca/2016/11/wechat-china-censorship-one-app-two-systems/

Ruby F, Goggin G and Keane J (2016) ‘Comparative silence’ still? Journalism, academia, and the five eyes of Edward Snowden. *Digital Journalism* 5(3): 353–367.

Rusbridger A (2017) Journalism after Snowden. In: Bell E and Owen T (eds) *Journalism after Snowden: The Future of the Free Press in the Surveillance State*. New York: Columbia University Press, pp. 21–28.

The Hong Kong Journalists Association (2017) Two systems under siege: Beijing turns the screws on Hong Kong media. Available at: https://www.hkja.org.hk/site/Host/hkja/UserFiles/file/Annual_report_2017.pdf

Tow Center for Digital Journalism (2015) Learning security: Information security education for journalists. Available at: https://towcenter.org/research/learning-security-information-security-education-for-journalists/

Tsui L (2003) The panopticon as the anti thesis of a space of freedom: Control and regulation of the internet in China. *China Information* 17(2): 65–82.

Tsui L (2015) The coming colonization of Hong Kong cyberspace: Government responses to the use of new technologies by the umbrella movement. *Chinese Journal of Communication* 8(4): 1–9.

Villeneuve N (2008) Breaching trust: An analysis of surveillance and an analysis of surveillance and security practices on China’s TOM–Skype platform. Available at: http://www.nartv.org/2008/10/01/breaching-trust-tom-skype/

Walton G (2001) *China’s Golden Shield: Corporations and the Development of Surveillance Technology in the People’s Republic of China*. Montreal, QC, Canada: Rights & Democracy.

Wash R (2010) Folk models of home computer security. In: *Proceedings of the symposium on usable security and privacy*. Redmond, WA, 14–16 July, pp. 1–16. New York: ACM.

Waters S (2017) The effects of mass surveillance on journalists’ relations with confidential sources. *Digital Journalism* 6: 1294–1313.

Whitten A and Tygar JD (1999) Why Johnny can’t encrypt: A usability evaluation of PGP 5.0. *USENIX Security Symposium*. https://www.usenix.org/legacy/events/sec99/full_papers/whitten/whitten.ps

Wong KC (2008) A preliminary assessment of the Hong Kong interception of communications and surveillance ordinance. *Commonwealth Law Bulletin* 34(3): 607–621.
Zuboff S (2015) Big other: Surveillance capitalism and the prospects of an information civiliza-
tion. Journal of Information Technology 30(1): 75–89.

Author biographies

Lokman Tsui is an Assistant Professor at the School of Journalism and Communication of the Chinese University of Hong Kong (CUHK) where he researches free expression and Internet regulation. Before he returned to academia, he was Google’s Head of Free Expression in Asia and the Pacific.

Francis Lee is Director and Professor at the School of Journalism and Communication, CUHK. He is the lead author of Media, Social Mobilisation and Mass Protests in Post-colonial Hong Kong (Routledge, 2011) and Media and Protest Logics in the Digital Era: The Umbrella Movement in Hong Kong (Oxford University Press, 2018). He is also Chief Editor of The Chinese Journal of Communication and Associate Editor of Mass Communication & Society.
### Appendix 1

**Coding samples.**

| Sentences                                                                 | Operational definition                                                                 | Awareness | Category |
|---------------------------------------------------------------------------|----------------------------------------------------------------------------------------|-----------|----------|
| ‘This means we are prepared to have our communication overheard. This began in the 70s/80s, it is not related to technology’. | Surveillance seen as impossible to protect against. Inability to see technological improvements in terms of security. | Low       | Obfuscation |
| ‘When I was a reporter, on sensitive cases, we didn’t disclose the names in telephone, meeting, chatting with friends. For example, the person’s name is ABC, we will name him or her an alias, called D. D said that even being taped or overheard, especially when we worked overseas, using international telephone, was easily being hacked. So we would use code names we all understand’. | Using (exclusively) low-tech means to protect sources | Low       | Obfuscation |
| ‘But there is not much sensitive issue in Hong Kong, we don’t need to be too nervous when we are dealing with the source’. | Security seen as unnecessary, journalistic work seen as not sensitive. ‘I’ve got nothing to hide’ attitude. | Low       | Obscurity |
| ‘I have no such experience before. I don’t think I have any secrets. Therefore I’m not a target for hacking. I haven’t got worried about it before’. | Security seen as unnecessary, journalistic work seen as not sensitive. ‘I’ve got nothing to hide’ attitude. | Low       | Obscurity |
| ‘I think it is an attitude, not a skill. The attitude is to do your job well. That’s why I think it is a matter of awareness. They need to find a way to ensure safety … and be able to do your job at the same time. How would you try all means to accomplish this goal?’ | Security seen as necessary and signifying journalistic excellence. | High      | Opportunity |
### Appendix 1. (Continued)

| Sentences                                                                                                                                                                                                 | Operational definition                                                                                                                                  | Awareness | Category       |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|----------------|
| ‘You shouldn’t think “it is okay that my files are read.” You can’t have this kind of attitude. Awareness is what matters the most. Some people might think that the authorities are omnipotent, they can read anything they want. I can’t avoid them regardless of what app I use. Some people really think like that. I believe how they think matter more than what skill or app they use’. | Security seen as necessary and signifying journalistic excellence.                                                                                           | High      | Opportunity    |
| ‘Sometimes the boss would joke “even if the Chinese government does not read [our messages], the American government does. You think they don’t read your Gmail?” I would respond “yes, but I’d rather they were read by the American government. Or my Kakao were being watched by the Korean government. I just don’t want them to be read by the Chinese government”’. | Sophisticated awareness of surveillance. Ability to distinguish threats.                                                                               | High      | Opportunity    |
| ‘We try our best to avoid phone calls and emails. It’s much better, thanks to 3G, 4G … We used to use Gmail but since it was heavily cracked down, we’ve switched to instant messaging systems. We don’t have to use emails now. We actually explored many options to avoid using emails’. | Proactive attitude toward security.                                                                                                               | High      | Opportunity    |
| ‘We use our own way. We don’t trust the company’s IT department! Same thing in every company! [Laugh]’                                                                                                        | Proactive attitude toward security.                                                                                                           | High      | Opportunity    |
| ‘Yes, their awareness is poor. Resources will be provided after an attack, and it’s not costly, therefore I don’t blame on resources. If you ask me, I blame on the poor awareness’. | Organization perceived to have reactive attitude, sees security as unnecessary cost.                                                                 | Low       | Obscurity (organization), opportunity (journalist) |
| ‘In my opinion, on one thing, it [the IT department] would not set up a VPN for China reporting team. Some news organizations have it but we don’t. Yes, they then set up one, but it didn’t work that well. I ended up buying another VPN just in case’. | Organization perceived to have reactive attitude, sees security as unnecessary cost.                                                                 | Low       | Obscurity (organization), opportunity (journalist) |
Appendix 2

Interview script

The interviews will be semi-structured and follow the general script below. The questions are designed to be open-ended and not to introduce bias or digital security concepts outright. For example, we want to avoid asking ‘do you use X security tool when communicating with sources’ and instead ask more general questions such as ‘do you do any special procedures for communicating with sources’.

Introduction

Demographics

1. How do you describe your professional status (newsroom, freelance, etc.)?
2. What media organizations do you work for?
3. What media have you worked in (print, radio, TV, online)?
4. What media do you currently work in (print, radio, TV, online)?

If more than one, please rank in order of frequency.

5. How many years have you been working as a journalist?
6. What is your educational background?
7. Do you have formal education in journalism?

If so at what level (e.g. undergraduate, graduate, apprenticeship)

8. Have you ever received training in physical security?
9. Have you ever received training in digital security?

Beat

1. What topics do you generally cover?
2. Do you consider any of your reporting areas to be sensitive?
   a. Can you tell us why you consider these areas sensitive (or not)?

Role in story creation

1. What is your role in creating or producing a story or article?
2. Walk me through the development of a typical news story you work on.
   a. How do you get from the start of things to publication?
   b. What are the steps and process?
   c. What technologies do you use?
3. 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.)
   a. How does this story compare to your typical source interactions?
Sources and info

1. What kinds of sources do you get your information from?
2. Why are these sources important for your work?
3. What is involved in finding these sources or them finding you?
4. Do you do anything special to communicate with sources?
   a. Do your procedures ever vary or change?
   b. If so, then how?
5. How do you store information provided to you by sources?
6. How do you disseminate/communicate information shared by sources?
7. Do you have any challenges obtaining information/locating sources?
8. How do you overcome these challenges?

Use of technology

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

Perceptions and experience with security threats

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

Training/organizational policy

1. Have you received, or implemented, practices to improve your source/data security?
2. Have you received any training for digital security in particular?
3. 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)?

4. Do you think that you have any challenges in how you secure yourself from digital threats?
   a. Probe this question on organizational and personal level.

5. Does your organization have any formal policies concerning computer security?

6. What support/capacities do you need for digital security that you do not currently have?