SOUNDING THE ALARM FOR “WATCHDOGS”:
THREATS TO JOURNALISTS’ DIGITAL SAFETY AND PROTECTION STRATEGIES

A Thesis
submitted to the Faculty of the
Graduate School of Arts and Sciences
of Georgetown University
in partial fulfillment of the requirements for the degree of
Master of Arts
in
Communication, Culture and Technology

By

Yaolin Chen, B.A.

Washington, DC
April 20, 2020
The research and writing of this thesis are dedicated to journalists who pursue truths with life-long efforts

Many thanks, Yaolin Chen
# TABLE OF CONTENTS

Chapter 1. Introduction .................................................................................................................. 1  
  1.1. Objective ................................................................................................................................. 1  
  1.2. This Thesis ............................................................................................................................... 2  

Chapter 2. Literature Review ......................................................................................................... 6  
  2.1 Consequence of Digital Surveillance and Malware Attacks on Journalists ........................... 7  
  2.2 Means of Digital Surveillance and Malware Attacks on Journalists ..................................... 12  
  2.3 Factors Contributing Journalists’ Vulnerability to Digital Surveillance and Malware Attacks .... 18  
  2.4. Journalists’ Strategies for Digital Safety .............................................................................. 25  
  2.5. Existing practices by other stakeholders ............................................................................ 29  
  2.6. Chapter Summary ................................................................................................................. 35  

Chapter 3. Methodology, Hypothesis, and Analysis ....................................................................... 37  
  3.1. Research Questions ................................................................................................................ 37  
  3.2. Methodology .......................................................................................................................... 38  
  3.3. Hypothesis and Justification ................................................................................................. 40  
  3.4. Analytics and Finding .......................................................................................................... 43  
  3.5. Chapter Summary ................................................................................................................. 48  

Chapter 4. Discussion .................................................................................................................... 51  
  4.1. How Do Journalists Protect Their Digital Safety? ............................................................... 51  
  4.2. What Influences Journalists’ Use of Digital Protective Measures? ...................................... 53  
  4.3. What Challenges Do Journalists Face in Their Efforts to Protect Their Digital Safety? ....... 54  

Chapter 5. Conclusion .................................................................................................................... 59  
  5.1. Key Takeaways of This Study ............................................................................................... 59  
  5.2. Recommendations ............................................................................................................... 61  
  5.3. Limitations ............................................................................................................................ 66  

Appendix I. Glossary .................................................................................................................... 69  

Appendix II. Survey Questionnaire ............................................................................................... 70  

Works Cited .................................................................................................................................. 73
LIST OF TABLES
Table 1. Beats and Frequency of Using Digital Protection ........................................ 44
Table 2. Media Format and Frequency of Using Digital Protection.......................... 44
Table 3. News Type and Whether Cybersecurity Training Is Helpful ..................... 45
Table 4. Media Format and Frequency of Using Digital Protection.......................... 45
Table 5. Positions and Frequency of Using Digital Protection ................................. 46
Table 6. Technical Skills and Frequency of Using Digital Protection ......................... 47
Table 7. Region and Frequency of Using Digital Protection ...................................... 47
Table 8. Gender and Frequency of Using Digital Protection ...................................... 48
Table 9. Newsroom Types and Journalists’ Access to Cybersecurity Training ......... 48
Table 10. Journalists’ Use of Digital Protective Measures ......................................... 51
Table 11. Journalists’ Frequency of Using Digital Protective Measures ..................... 52
Table 12. Journalists’ Use of Digital Protective Measures ......................................... 55
Table 13. Whether Journalists’ Newsrooms Provide Cybersecurity Training .......... 56
Table 14. Whether Journalists’ Newsrooms Provide Cybersecurity Training .......... 56
Table 15. Whether Journalists’ Newsrooms Provide Cybersecurity Training .......... 57
Table 16. Formats of Cybersecurity Training Offered by Newsrooms ..................... 57
Chapter 1. Introduction

1.1. Objective
Journalists are considered as “watchdogs” of our society. They collect, verify and disperse information via investigations and publications, and thus, they bring issues to spotlights and keep the government power in check. In the digital era, advanced technology created more opportunities for “watchdog” journalism. It has generated online and digital media formats, and has presented journalists new ways of gathering information, communicating with source, creating and distributing stories (Çatal 2017; International Center for Journalists 2019). But it also provides easy access for digital surveillance and malware attacks on journalists.

In various parts of the globe new technology has become a powerful tool for governments and non-benevolent actors to track the physical movements of journalists and their sources. Digital devices allow easy access to the digital communication of journalists on a daily basis, and therefore collect data on their work and personal identities. Internet services, including social media, emails and messaging, also expose their activities to the oversight of governments and other malicious actors (Digital Rights Foundation 2017; Waters 2018). These means of digital surveillance, which intersect with malware attacks at time, have posed threats to journalists’ personal safety and generated a far-reaching consequence. Journalists and newsrooms are inclined to censor their news content, and therefore result in the violation of freedom of speech (Waters 2018; Tsui and Lee 2019). Digital surveillance also causes breaches of civil rights, including privacy and digital rights. Meanwhile, it could limit journalists’ ability to keep government power in check. As journalists’ role as “watchdog” could be compromised, the
sustainability of political democracy could be challenged (Mills and Sarikakis 2016). The situation of “watchdog” journalists is alarming.

1.2. This Thesis

This thesis has two goals: (1) to inform people of the alarming situation of journalists’ digital safety, including the far-reaching consequences of digital surveillance and malware attacks on journalists, journalists’ vulnerability to digital threats, and how their lack of protective compounds their potential vulnerability; (2) to provide journalists and their new agencies with updated information and practical recommendations to shield themselves from digital surveillance and malware attacks. To achieve these two goals, I develop my thesis into the five chapters so as to discuss the protection of journalists’ digital safety globally.

1.2.1 Thesis summary

I will present the topic background and the framework of my thesis in Chapter 1. I will also provide a review of the extant literature in Chapter 2. Governments and malicious social actors used digital surveillance and malware attacks to generate a “chilling effect” on journalism. Extant literature shows that digital surveillance and malware attacks on journalists have posed threats to their personal safety and generated far-reaching erosion of civil rights, freedom and democracy. It also explains factors contributing to digital surveillance and malware attacks on journalists, including newsrooms factors, social and legislative contexts. I will also examine the existing measures taken by journalists to secure their data, as well as the current practices established by various stakeholders. These stakeholders, mostly newsrooms, journalist communities and law makers have been taking efforts to protect the digital safety of journalists, yet their practices have limitations. I will analyze these limitations based on the extant literature.
Following the literature review, I will explain my methodology and analyses in Chapter 3. I used the 2019 State of Technology in Global Newsrooms survey as my data source and conducted data analyses based on the survey data. I examined five hypotheses via crosstabs, and two hypotheses via frequencies. My key findings are astounding. Over 65% of journalists never or rarely used digital protection, including journalists in vulnerable groups, such as female journalists, politics or crime reporters. But the lack of digital protection is not the only cause to exacerbate journalists’ vulnerability to digital surveillance and malware attacks. The lack of organizational training offered by their newsrooms, also challenge their efforts to secure their data, sources and devices, as my analyses show that only 7.6% of newsrooms offer cybersecurity training. In chapter 4, I am going to discuss how my analyses answer three of my research questions. In light of my key findings, I will conclude my thesis with the key takeaways in Chapter 5. This chapter will also offer my recommendations for journalists and other stakeholders to shield journalists from digital threats, as well as directions for future studies.

1.2.2. Research question

I achieve these two goals by investigating the following questions:

RQ1: How do journalists ensure their digital safety?

RQ2: What influences journalists’ use of digital protective measures?

RQ3: What challenges do journalists face in their efforts to ensure their digital safety?

1.2.3. Hypothesis

While exploring my research questions, this thesis examines the following hypotheses:

H1: Journalists’ use of digital protection is closely related to their news content. Journalists who cover sensitive beats are more likely to use digital protection frequently. Journalists who cover local news are unwilling to secure their data.
H2: Media formats influence journalists’ frequency of using digital protection. In general, journalists working with online media are most likely to use digital protection frequently. Among legacy news outlets, printed newspaper and television journalists are more willing to protect their digital safety compared with their counterparts in radio or print magazines.

H3: Journalists’ own positions in their newsrooms influence the frequency of their use of digital protection. Full-time and investigative reporters are at higher rates to secure their data more frequently than their editors and freelance peers.

H4: Journalists’ own positions in their newsrooms influence the frequency of their use of digital protection. Full-time and investigative reporters are more likely to secure their data more frequently than their editors and freelance peers.

H5: The region in which journalists work influences their frequency of using digital protection.

H6: Female journalists are less likely to use digital protection than their male peers.

H7: Journalists’ access to cybersecurity training varies based on types of their newsrooms.

1.2.5. Contribution
At this point there is little empirical data or literature available that has examined how newsrooms factor, social or legislative context affect journalists’ decisions to use digital protection. Existing literature shows that certain factors, such as the news content that journalists cover most often, their positions in newsrooms, gender or minority identities, influence the likelihood of journalists to take protective measures. But most findings were discovered through qualitative interviews. They do not show statistical relationship between these factors and journalists’ use of digital protection. The extant literature also reveals the commonly used digital protection amongst journalists. But the existing information is not enough to know about their choice of certain protection, and their frequency of using a certain protection. There is not empirical data to show which digital protection is the most commonly used.
Existing normative or legal frameworks neither provide a comprehensive view of how journalists' vulnerability may be compounded by newsroom factors, social or legislative contexts. These frameworks also somewhat outdated. For example, the UN plan were based on two studies prior to 2017, “Building digital safety for journalism: a survey of selected issues” (Henrichsen, Betz, and Lisosky 2015) and “Protecting Sources in the Digital Age” (2017). In addition, these frameworks are not legally binding. They neither provide mandatory requirements for news organizations to enforce, nor grant legal remedies for journalists confronted with digital threats.

To fill this gap, this thesis will provide:

• A social-technical analysis of the consequences caused by digital surveillance and malware attacks. The consequence will be discussed from the perspective of journalists and their newsrooms, but also the perspective of civil rights, freedom of speech and political democracy.

• Latest information on journalists’ choice of any digital protection, including encrypted emails and messaging, secure audio or video calls, and VPN. The information will explain how frequently each of these protections is used, and therefore illustrate the most commonly used protection in the recent period.

• A statistical analysis on various factors contributing to journalists’ decisions to use digital protection. This statistical analysis will be synthesized with extant literature to identify vulnerable groups across journalists’ communities.

• Provide directions for future studies to understand the various challenges with which journalists are confronted in their efforts to protect their digital safety, and journalists’ motivations to choose a certain digital protection.
Chapter 2. Literature Review

The existing literature shows that most of the real and potential threats to journalists’ digital safety resulting from digital surveillance. The real threats refer to a situation that journalists’ personal safety is compromised by digital surveillance (Henrichsen, Betz, and Lisosky 2015), such as being followed, blackmailed, arrested or even murdered. Potential threats are based on an assumption by journalists that their digital communication is always being surveilled by the states or malicious actors (Water 2018). These assumed threats could compromise journalists’ mental health (Digital Rights Foundations 2017).

In regard to surveillance, journalists define this word as an act of “watching” (Waters 2018)” and “monitoring” (Waters 2018: 3). They identify it as the feeling of being observed by someone hidden in the dark (Digital Rights Foundation 2017). In the case of digital surveillance, it is a process of “monitoring, intercepting, collecting information” (Henrichsen, Betz, and Lisosky 2015: 22), and activities of storing and preserving the intercepted information (Henrichsen, Betz, and Lisosky 2015: 22). The most famous example is the Snowden files, which revealed the National Security Agencies’ (NSA) surveillance of civilians and civil parties (Waters 2018). Meanwhile, malware attacks against journalists have also become a serious issue. The existing literature also shows that malware attacks have been used as a means to facilitate digital surveillance of journalists by state and malicious actors (Henrichsen, Betz, and Lisosky 2015). For example, governments and malicious actors inserted spyware (Sant 2018; Kenyon 2018) or launch phishing attacks (Henrichsen, Betz, and Lisosky 2015) on journalists’ devices to intercept and detain their data.

In addition, existing literature explores the consequences and prevalent means of conducting digital surveillance and malware attacks on journalists. By reviewing previous studies, I
discovered that various way of conducting digital surveillance and malware attacks. Later in the chapter, I will investigate how existing literature shows the how newsroom factors and social or legislative contexts could exacerbate journalists’ vulnerability to digital surveillance and malware attacks. In addition to these factors, journalists’ strategies of digital safety determine their decisions to use digital protection which enhance or compound their vulnerability. These protection measures include the use of encrypted emails and messaging, company sponsored or personal VPN, and secure document storage, which requires the individual efforts of journalists (Henrichsen, Betz, and Lisosky 2015). However, the protection of journalists’ digital safety cannot solely rely on individual efforts. I will refer to the literature for existing normative and legal frameworks established by international organizations and policy makers, toolkits and training offered by the global journalist community and newsroom.

2.1 Consequence of Digital Surveillance and Malware Attacks on Journalists

In this section, I am going to review how the existing literature discusses the consequences of digital surveillance and malware attacks on journalists. Digital surveillance and malware attacks can result in offline following, harassing, torturing, imprisoning, and even murdering, which compromise journalists’ personal and professional safety. Digital surveillance of journalists has exerted a “chilling effect” (Bradshaw 2015; Mills and Sarikakis 2016; Mills 2019), which carries two different meanings. First, journalists are prone to become vigilant about their activities and digital communication. Second, journalists tend to censor themselves to avoid covering certain sensitive, contentious, and conspicuous topics (Waters 2018; Tsui and Lee 2019). As a result, journalists tend not to cover these topics, which could trigger the erosion of freedom of speech. This situation will squeeze the space for “watchdog” journalism to talk about sensitive topics relevant to civil rights and government power. Therefore, the role of “watchdog” journalism to keep government power in check in compromised. This is to say, digital surveillance and
malware attacks on journalists have generated far-reaching consequences for freedom and democracy (Mill and Sarikakis 2016).

2.1.1. Threats to journalist personal safety

Digital surveillance has contributed to the increasing threats to journalists’ personal safety. The advanced technology of digital surveillance and malware attacks provide an increasing ease for governments and malicious actors to spy on journalists and therefore collect, detain and store data on their work activities and digital communication with their sources. These actors have also been using location tracking and facial recognition to monitor IP addresses and physical movements of journalists and their sources (Henrichsen, Betz, and Lisosky 2015; Digital Rights Foundation 2017).

In various parts of the globe new technology has become a powerful tool for governments and non-benevolent actors to track the physical movements of journalists and their sources. Internet services, including social media, emails and messaging, also expose their activities to the oversight of governments and other malicious actors (Digital Rights Foundation 2017; Waters 2018).

Mills (2019) believed that the threats to journalists, caused by digital surveillance and malware attacks, vary across democracies and oppressive or authoritarian regimes. In Western democracies, such as the U.S., U.K., and Italy, digital surveillance of journalists is often accompanied by blackmailing, on-the-ground following, or frequent interrogation (Mills and Sarikakis 2016; Water 2018). In Mills and Sarikakis’ study, journalists who published news stories on the Snowden files, including reporters in a British newspaper “the Guardian”, were confronted with intensive surveillance of their digital devices, as well as frequent interrogation by the law enforcement. At the same time, Mills (2019) believed that the situation was very severe in oppressive and authoritarian regimes such as Egypt, Turkey, Rissa and Iran. In these
regimes, the freedom of press was suppressed, and independent watchdog journalism did not exist. Journalists’ data was obtained via digital surveillance, and their data was often used to arrest, detain or charge them. In fact, covering national security stories could lead to the imprisonment of journalists themselves. Sometimes, the surveillance leads to the murder of journalists. During the civil war, Syria journalists “face death, kidnapping, torture, and arrest by both state and rebel forces” (Mills 2019: 16). Another prominent example is the Saudi Arabic journalist Jamal Khashoggi. Two months before Khashoggi was murdered inside the Saudi Embassy in Turkey, his encrypted messages were tapped by the Saudi government (Sant 2018; Kenyon 2018). His example also shows how malware attacks become a means for surveilling journalists. These examples show that digital surveillance and malware attacks pose threats to journalists’ personal safety and loom over their professional environment.

2.1.2. Cautiousness and mental issues

Because of the threats that happened to some journalists, the rest of their peers have experienced a chilling effect. They are alerted to the possibility of being surveilled and threatened. As a result, some of them are exposed to a risky professional environment, which may force them to quit their jobs. For those who continue their journalistic career, they have become cautious about their digital communication, and they have established complicated workflows to increase the use of digital security tools (Waters 2018) and have avoided digital communication whenever possible (Mills and Sarikakis 2016; Milosavljević, Prodnik, and Kučić 2015). For example, they prefer to have a face-to-face meeting with their sources and colleagues in spaces with loud background noises and no digital devices (Mills and Sarikakis 2016; Milosavljević, Prodnik, and Kučić 2015; Waters 2018). Additionally, journalists exchange information through paper or devices disconnected from the Internet (Mills and Sarikakis 2016; Milosavljević,
Prodnik, and Kučić 2015; Posetti 2014), and they do not bring digital devices with them when crossing a country border (Mills and Sarikakis 2016).

In addition to cautiousness, journalists are haunted by paranoia, fear and trauma caused by digital surveillance, and these feelings may exacerbate their mental health issues (Digital Rights Foundation 2017). The paranoia of being surveilled by the “big brother” has penetrated into the personal lives of some journalists. They always assume that their conversations are being listened to or information being intercepted, even if their personal lives are completely disconnected from their job. Accompanied by the paranoia, they are trapped in a feeling of powerlessness that they have lost control of their life and cannot escape the paranoia of always being watched (Waters 2018). The report from Digital Rights Foundation (2017) also reveals that digital surveillance caused a feeling of fear and shame, with which journalists were haunted. Due to the lack of a supportive culture for discussing and addressing digital surveillance and cyberattack across global journalist communities, journalists have to address the issues and traumas of digital surveillance or malware attacks themselves. This compounds their mental health issues.

2.1.3. Self-censorship of journalists and newsrooms

With regards to the threats to their personal and professional safety caused by digital surveillance and malware attacks, journalists also tend to self-censor themselves. The studies of Digital Rights Foundation (2017), Waters (2018) and Tsui and Lee (2019) discussed how journalists and their newsrooms circumvent certain sensitive, conspicuous or controversial topics to avoid being surveilled, attacked or threatened. These topics include national security, religion, gender issues, government corruption, human rights violations, police policies, military, and foreign ministry affairs. Journalists and their newsrooms tend to restrict themselves to cover these sensitive, conspicuous or controversial topics. One example is that some journalists in East Asia would at times drop their stories in concern of the threats caused by digital surveillance (Tsui and Lee
Another example is the female journalists in Pakistan reported that they avoid talking about national security or religious issues on television programs or their personal Twitter or Facebook accounts (Digital Rights Foundation 2017). These examples show that self-censorship limits journalists’ and their newsrooms’ abilities in covering topics that are vital to civil rights and democracies.

2.1.4. Erosion of civil rights and democracy

As referred to in the section above, the self-censorship of journalists and their newsrooms resulting from the digital surveillance exerts a negative impact on civil rights and democracy. To understand this claim, it is important to explore the context of mass surveillance and the role of civil society and “watchdog” journalism in democracy which are explained in the study of Mill and Sarikakis (2016).

The capability of state surveillance, including digital surveillance of journalists, has been expanded by national security laws in the past two decades. Governments of the U.S, U.K., France, Germany, and Poland, have passed laws that allow law enforcement to expand their scale of surveillance to civilians and civil parties. This claim of Mill and Sarikakis is supported by the example provided by Waters’s (2018) study that law enforcement in the U.S. can request access from internet service providers, such as telecommunications companies, search engines, and social media platforms, which collected and detained users’ data for national security purposes. This mass surveillance has violated civil rights, such as freedom of speech as well as privacy and digital rights. Meanwhile, it has expanded government power by increasing the vulnerability of civil society to state surveillance. As a result, the role of civil society to keep the power balance in a democratic society may be weakened. This situation may pose a challenge to the sustainability of political democracy (Mill and Sarikakis 2016).
In a situation as alarming as this one, journalists are obligated to serve as a “watchdog” of
government power, which requires them to bring the issue to the news spotlight and therefore
keep the government power in check. However, the digital surveillance of journalists has
resulted in self-censorship, which limits their activities and reporting on the issue of mass
surveillance. As Fonbuena (2017) believed, internet service companies including
telecommunication providers, search engines, and social media platforms – are compromised by
national security and anti-terrorism legislation, and thus journalists are deprived of legal ways to
protect their sources. Therefore, digital surveillance has also restrained whistle blowers to work
with journalists on the issues of digital surveillance (Waters 2018). This is to say, the digital
surveillance and malware attacks on journalists and their sources has generated a chilling effect,
which prevents “watchdog” journalism to sound the alarm for the public on the expansion of
government power, the violation of civil rights, and the erosion of freedom and democracy.

2.2 Means of Digital Surveillance and Malware Attacks on Journalists

The existing literature shows that the actors employing digital surveillance are diverse. They
are usually entities that have a certain extent of authority, such as government, law enforcement,
or business entities (Waters 2018), terrorist groups or crime organizations or internet users that
have different religious, political, and cultural beliefs from the surveilled journalists (Digital
Rights Foundation 2017). These actors carry out digital surveillance of or malware attacks
against journalists in various ways, such as data collection and detainment on cloud databases,
malware attacks by inserting malware and manipulating journalists’ devices, and social media
surveillance (Henrichsen, Betz, and Lisosky 2015; Digital Rights Foundation 2017; Waters
2018). Through my research, I discovered that malware attacks could become a means of
conducting digital surveillance of journalist, which is exemplified by the use of the Remote
Control System and Pegasus. This will be further explained in this section.
2.2.1. Digital surveillance of journalists

Existing literature shows that governments in western democracies have been surveilling civilians and civil parties, including journalists in various ways. One prevalent way is to collect, detain, and analyze the users’ data from internet services providers (ISPs), including cloud computing, digital communication, social media and mobile applications providers. The collected user data includes personally identifiable information (PII), user activities and digital communication data (Mills and Sarikakis 2016; Waters 2018; Mills 2019).

PII is information that consistently links to a certain person and provides a thread for a third-party to locate the person. Some examples of PII include, but are not limited to: (1) name and birthdate information; (2) personal identification and property numbers, such as social security number; (3) address and contact numbers; (4) biometric data including retina, voice, fingerprints or facial recognition; (5) online asset information exemplified by Internet Protocol (IP) or Media Access Control (MAC) addresses (Joseph). Further information will be demonstrated in the following paragraph.

The capability of mass surveillance has been expanded globally by both technical and legislative means. After the 9/11 attack in U.S., various countries have enacted laws allowing law enforcement to request for users’ data of social media and digital communication tools in the name of national security investigation, including state departments in the United States, United Kingdom, Germany, Poland, and France (Waters 2018; Mills and Sarikakis 2016; Prodnik, and Kučić, 2015; Posetti 2017). In 2013, Edward Snowden revealed evidence of the surveillance carried out by the NSA. The NSA had been conducting mass surveillance of innocent civilians and civil parties and collecting their data (Waters 2018; Gellman and Poitras 2013). The NSA collected, detained and stored users’ data from emails, audio and video chats and documents retrieved from nine Internet companies, including Google, Apple, Microsoft, and Facebook.
(Gellman and Poitras 2013). WhatsApp also admitted that they allowed law enforcement to access and detain user data (Milosavljević 2015). Recently, Apple conceded its encryption plan for users’ data stored in Apple cloud server under FBI’s pressure (Menn 2020).

**Data mining and storing via cloud databases**

Nowadays software-as-a-service (SaaS), infrastructure-as-a-service (IaaS) and private cloud are three common cloud databases services. A cloud database is “a database service built and accessed through a cloud platform” that “enables enterprise users to host databases without buying dedicated hardware”, and “can be managed by the user or offered as a service and managed by a provider” (IBM). Cloud databases have become easy to access for third-party actors detecting, collecting and storing users’ personal identification and their communication data (Waters 2018) due to the following reasons.

First, most cloud databases do not raise their security level if there is sensitive data in their storage (Paul, Talreja, and Sahu 2012). Sensitive data can be exemplified as PII, which provide a clue for third-party actors to trace an individual, or data of private communication and confidential activities (Waters 2018). The data is oftentimes stored with common information, which is guarded by the lowest level of security (Paul, Talreja, and Sahu 2012).

Second, cloud databases have a low visibility “into what data is stored within cloud applications” (McAfee n.d.) and an inability to prevent malicious actors from accessing sensitive data (McAfee n.d). Thus, defense systems of cloud computing services are vulnerable to forced entry and malicious attacks on sensitive data stored in clouds.

**Data collection via internet service**

Existing literature shows that internet services providers (ISP), including cloud computing, digital communication, social media and mobile applications providers, have become easily accessible for government and malicious actors to collect and detain the data of civilians and
civil parties. The data include personally identifiable information (PII), user activities and digital communication data (Mills and Sarikakis 2016; Waters 2018; Mills 2019).

In addition to cloud computing, other internet services, such as digital communication, social media and mobile applications also increase the vulnerability of internet users, including journalists and their sources. This can happen by collecting users’ PII. For example, Facebook has been accused of secretly collecting and storing PII by developing and launching various mobile apps. These mobile apps are suspected of using location tracking, secret screenshot and recording, or voice assistance services to trace users without permission (Venkatadri et al. 2019). Meanwhile, these internet services can serve as a means to intercept digital communication and trace the activities of internet users. Google, for instance, had been tracing IP addresses of a hacktivist via its email service Gmail and recording his emails content under the request of U.S. law enforcement (Mills and Sarikakis 2016). Another example is the NSA program that collected and intercepted the data of digital communication, documents, and user activities from nine internet companies, including Google, Apple, Microsoft, and Facebook (Gellman and Poitras 2013; BBC 2014 in Mills and Sarikakis 2016).

**Surveillance of social media**

Social media can increase journalists’ vulnerability by providing access to journalists’ sensitive data or opening a way for the state and malicious actors to surveil journalists. Social media has become a major source of PII. Social media sites, such as Facebook, LinkedIn and Twitter, require users to provide PII, such as full name, phone number, education and employment histories, and profile pictures. This information will be entered, stored, and controlled in the databases of the service providers. These social media services can also track and record users’ activities with GPS location tracking, cookie, and browsing history (Joseph n.d.). Meanwhile, a stranger can access the PII displayed on users’ profile via search engine or
direct access to users’ social media accounts, which are mostly public domains accessible to anyone (Hasib 2009; Digital Rights Foundation 2017).

Meanwhile, the public nature of social media accounts also allows the states and malicious social actors to gather the content posted without tracing journalists’ PII. This kind of social media surveillance is often accompanied by online abuse by social malicious actors as well as on-the-ground surveillance and blackmailing (Henrichsen, Betz, and Lisosky 2015). Digital Rights Foundation (2017) reveals that some Pakistanis journalists reported that some internet users warned them of their “inappropriate” speech on Facebook pages or Twitter. Some other journalists also received warnings from the law enforcement that their posts on social media were being watched and recorded.

2.2.2. Malware attacks

Government and malicious actors have been using malware to launch digital attacks and manipulate the encrypted and obfuscated internet use of internet users. These malwares are developed by commercial entities. Some of the prevalent malware attacks are remote control, proxy servers or media malware, phishing, denial of service, or man-in-the-middle attacks. In fact, several examples in this section show that malware attacks frequently serve as a means for governments to conduct digital surveillance of journalists.

**Remote control spyware**

Remote control spywares enable unauthorized devices or servers to control a device remotely. Once these spywares are inserted through phishing emails or attachments they could allow attackers to “open documents, download software, and even move the cursor” around users’ screen on a real time basis (Andrew Heinzman 2019). One of the most popular remote-control spywares is the Remote Control System (RCS). This product inserts malicious programs allowing surveillants to remotely hack and control targeted devices. The software is developed
by the Hacking Team Company, and exclusively sold to governments globally. In 2014, the Citizen Lab listed the countries in which government entities are using the RCS as a way to surveil journalists. The document also included a report that several Ethiopian journalists were targeted by the state with the RCS (Poetranto 2014; Marczak et al. 2014A).

**Malicious proxy servers and media spyware**

Proxy servers are used by government operators to obscure their identities. These servers enable spyware to send the hacked data from the targeted device to the end point server the government operates through third countries without being traced (Marczak et al. 2014B). Media spyware such as Pegasus, developed by the Niv, Shalev and Omri (NGO) Group, is sold to governments for intercepting contents of phone apps and calls, opening the camera and microphone on the device remotely (Kenyon 2019). Pegasus was used to target several journalists before they were murdered, including Jamal Khashoggi. Jamal’s friend had been sent “a malicious link to the spyware”, which intercepted his encrypted messages with Khashoggi. One of his friends believed that the intercepted content was related to the murder of Khashoggi, which happened two months later (Sant 2018; Kenyon 2018). This is another example to show how malware attacks could provide an access for states to spy on journalists.

**Phishing and fake domain attacks**

Phishing malware is often used with fake domains to launch digital attacks on journalists. It uses phishing links or attachments to bait journalists to malicious websites that are disguised as legitimate sites. These websites are also called “fake domains.” Senders of phishing links and attachments usually disguise their accounts by using similar numbers or addresses of journalists’ colleagues, friends or other acquaintances (Henrichsen, Betz, and Lisosky 2015; Marquis-Boire 2012; Carbone 2013). Once journalists open phishing links or attachments, other malwares, such as remote-control spywares, could be downloaded and inserted on their devices to collect, steal
or manipulate their data. One famous phishing malware is Remote Access Trojan (RAT) (Henrichsen, Betz, and Lisosky 2015).

**Man-in-the-middle (MitM) attack**

Some attackers insert themselves into the digital connections of journalists with websites to intercept information. One common way is to use a WIFI router disguised as legitimate WIFI connections, such as free public WIFI hotspots. Another way is to insert malicious code in the browser of a target user to secretly collect data exchanged between the browser and target websites.

**Denial of service attacks (DoS)**

Denial of service attacks is a tactic to prevent legitimate users from accessing the websites by using a high volume of traffic to paralyze the targeted hosts or networks (U.S. Department of Homeland Security 2019). By blocking legitimate access, DoS serves as means of direct censorship on the content. This is because it prevents data from “being disseminated and viewed…may result in financial loss to the online media actors because they have been taken offline and their audience is unable to access the website loss of media actors” (Henrichsen, Betz, and Lisosky 2015: 27).

### 2.3 Factors Contributing Journalists’ Vulnerability to Digital Surveillance and Malware Attacks

Journalists in various groups have different vulnerabilities to digital surveillance and malware attacks. Their vulnerability varies based on various contexts in newsrooms, including the news content they cover, their media formats, types of their newsrooms, and their positions in their newsrooms. Meanwhile, social and legislative context also affect journalists’ vulnerability. In South Asia, certain social identities, such as religion, class, and political background, intersect with gender to compound the minority of these female journalists (Digital Rights Foundation 2017). Besides, legislative contexts such as laws and policy at times limit
journalists’ activities and their choices of digital protection. The state surveillance has been legalized by the national security laws, and journalists become victims of the surveillance. Meanwhile, VPNs are prohibited in countries such as China and Russia, limit the choice of journalists located at these countries to use digital protection (Henrichsen, Betz, and Lisosky 2015; ProtonVPN).

2.3.1. Journalists’ vulnerability and newsroom context

To understand journalists’ vulnerability to digital surveillance and malware attacks, we need to understand the definition of journalists. According to the Human Rights Committee of the United Nations (UN), journalism is a function “regularly engaged in the collection and dissemination of information to the public”, which is undertaken by full-time professionals working for print media or by bloggers publishing their own content online “regardless of whether they are formally recognized as a “journalist” by their government” (Article 19 2017). This definition recognizes the evolving nature of journalism, which includes journalists working for new media, such as news websites, news apps or blogs, on either full-time, part-time or freelance basis (Digital Rights Foundations 2017). It also includes internet users who utilize social media to disclose the government’s human rights violations, advocate for democratic movements and social change, or do fact-checking themselves, and gradually become citizen journalists (Henrichsen, Betz, and Lisosky 2015).

By revisiting the definition of journalists, we are able to realize that nowadays the broader meaning of journalism may reflect the various contexts in newsrooms that affect journalists’ vulnerability. In the following paragraphs, I am going to review the extant literature which describes how journalists’ vulnerability varies based on the news type and beats they cover, their media format, types of their newsrooms, and their newsroom positions.
News type and beats

Journalists’ vulnerability to digital surveillance can directly result from the sensitivity of their topics. When covering highly sensitive, contentious or conspicuous issues, journalists and their sources are very likely to be surveilled. These issues including national security, terrorism, surveillance and intelligence agencies and organized crimes, state violence, governmental actions, police, military or foreign policy, religious controversies and so on (Mills, 2019; Digital Rights Foundation 2017; Mills and Sarikakis 2016; Waters 2019; Tsui 2019). For example, journalists in Hong Kong reported that they may face censorship on their WeChat communication when covering issues that related to Chinese politics (Tsui and Lee 2019).

Media format

The existing literature shows that media format and newsroom types, which are sometimes defined by the media formats, affects the vulnerability of a journalist. In general, online media journalists are more vulnerable than their peers working at legacy news outlets. According to the Committee to Protect Journalists (CPJ), 698 journalists were sent into imprisonment from 2013 to 2018, and 61% of the imprisoned journalists were working for online media (Committee to Protect Journalists 2019). Still, journalists working with legacy news outlets, newspaper and radio journalists reported a more severe digital surveillance than their peers (Digital Foundation 2017). One example is the state surveillance on journalists working for the Guardian, a British national newspaper can also prove this tendency, as mentioned in the previous chapter (The Guardian 2013 in Mills and Sarikakis 2016). Besides, journalists in South Asia are more likely to receive better protection of their digital safety if their newsroom is a local branch of an international news organization. This is because these newsrooms usually offer systematic support for journalists to protect their digital safety, such as a cyber security department to provide cybersecurity tools and training (Digital Rights Foundation 2017).
**Journalists’ newsroom positions**

Digital Rights Foundation (2017) reported that journalists are more vulnerable than their editors, because their job requires exposure on the spot or to the public and direct contacts with confidential sources. In contrast, editors tend to do their job behind the scenes. By the same token, investigative reporters are also more likely to be confronted with digital surveillance compared to other reporters. This is also because investigative reporters cover sensitive, contentious and conspicuous topics most often (Waters 2018; Milosavljević, Prodnik, and Kučić 2015). Meanwhile, journalists working part-time and freelance are likely to suffer more threats of digital surveillance than their full-time peers, because they receive less protection from the new organizations than full-time employees (Digital Rights Foundations 2017).

**Technical skills**

Journalists’ competency in computer skills also affects their use of digital protection. Waters (2018) found that journalists are more likely to use digital protection if they are familiar with computer knowledge because they are more aware of the threats and consequences of mass surveillance of civilians and civil parties. Thus, journalists who have less familiarity with computer skills may be more vulnerable because they are lacking in knowledge and awareness of how to protect their digital safety.

In sum, several factors in newsroom context influence journalists’ vulnerability to digital surveillance and malware attacks: the news content they cover often, media format, newsroom types and technical skills. In addition to their vulnerabilities, these factors may influence their use of digital protection, which I will further examine in my study.

**2.3.2. Journalists’ vulnerability in social-cultural and legislative context**

Journalists are surveilled not only due to the nature of their jobs, but also because of the social and legislative contexts to which they are connected. Most of the time, social-cultural contexts are more related to journalists’ social identities, such as their gender or religious, ethnic,
class or political identities. While the impact of social-cultural contexts is more subtle, legislative contexts more directly determine journalists’ vulnerability to digital surveillance and malware attacks. Legislative contexts often are related to the enforcement of state surveillance, censorship or internet control which is established on the ground of the laws or regulations in a certain region.

**Social-cultural context**

The intersection of gender and various social-cultural contexts, including ethnic, religious, political identities or classes, could compound the vulnerability of journalists. According to the UN, female journalists are more vulnerable to digital surveillance compared to their male counterparts. They are subject to “gender-based” threats or attacks that are defined as those “disproportionately experienced by women journalists, in particular sexual and gender-based threats” (Article 19 2017:10). This has become a global issue. Globally female journalists reported that “online attacks have become more visible and coordinated” from 2014 to 2019 (International Women’s Media Foundation 2018). In North America, 85% of female journalists believed the environment had become less safe for them from 2017 to 2019 (Westcott 2019). Female journalists in Pakistan also reported the digital surveillance on them was based on a deeply rooted stereotype that they are less competent compared with their male counterparts (Digital Rights Foundation 2017). The following paragraph will offer detailed reasons to explain how the intersection of gender and other social-cultural contexts could compound the vulnerabilities of female journalists.

There are several reasons for the vulnerability of female journalists. First, some attackers regard female journalists as sexualized objects; as a result, some attacks are based on their personal identities. For instance, female journalists received sexist comments on their appearance and personal life or were blackmailed to disclose sensational details of their personal life to the
public (Digital Rights Foundation 2017). These sexual threats could become violent, such as “threats of rape or other violence toward female journalists and their families” (Henrichsen, Betz, and Lisosky 2015: 45).

Second, digital surveillance of female journalists, which is accompanied by online abuse or attacks, is based on a stereotype that women are not competent in journalism (Henrichsen, Betz, and Lisosky 2015; Article 19 2017). For example, some journalists in Pakistan were told by government officials, who were conducting digital or social media surveillance of them, that they were conducting digital surveillance as a state protection for women. Sometimes they should not work on topics that were not appropriate for women to cover (Digital Foundations 2017). These are some of the examples to show that digital surveillance on female journalists are based on gender stereotypes, which are held by attackers who are “motivated wholly or in part by the mere fact of a journalist being a woman” (Article 19 2017:10).

Third, the backgrounds of religious or ethnic minorities could compound female journalists’ vulnerabilities. Compared to other female journalists, female journalists from these certain backgrounds are more vulnerable to digital surveillance and the online abuse caused by it. The data from Amnesty International and Element AI (2018) indicates that female journalists of color or minority ethnics, such as black, Asian and Latino, were 34% more likely to be targeted in online abuse on Twitter compared to white female journalists. In South Asia, these identities may provoke comments such as “your head is uncovered” or “half-breed” (Digital Rights Foundation 2017: 19-20).

Fourth, female journalists who worked with news organizations that have a specific political position, either left or right leaning, were vulnerable to online abuse (Westcott 2019). For example, female journalists reported that they faced severe attacks due to “a rise of nationalism
around the world and the use of digital networks to thwart political processes" (International Women’s Media Foundation 2018).

Fifth, female journalists are lacking in protective resources, such as cybersecurity training and a reporting or discussion mechanism (Westcott 2019; Digital Rights Foundation 2017). This compounds their vulnerability. For example, less than 40% of female journalists in North America, such as Canada and the U.S., received safety training, including cybersecurity training that ensures their digital safety (Westcott 2019). In addition to cybersecurity training, female journalists in Pakistan also complained that their newsrooms and communities did not encourage them to either share their experience with digital surveillance and online abuse, nor to discuss the possible strategies to ensure their digital safety (Digital Rights Foundation 2017).

Sixth, the social-cultural contexts in certain regions could compound the vulnerabilities of female journalists located in these regions. For instance, Pakistani women are obstructed by this social stereotype and therefore there are not many female journalists. The scarcity of female journalists makes the rest of them more noticeable by law enforcement and other malicious actors (Digital Rights Foundation 2017).

Given the aforementioned information, female journalists could be more vulnerable to digital surveillance and online abuse compared to their male counterparts. In fact, female journalists are confronted with bias-motivated and gender-based attacks, and they are lacking in protective resources to secure their data.

**Legislative context**

Furthermore, legislative contexts, such as national security laws, censorship and internet control compound journalists’ vulnerability by legalizing mass surveillance or limiting their choice of digital protection. Governments’ capacities for conducting mass surveillance have been expanded by national security laws in western democracies (Mills and Sarikakis 2016), as
discussed in the previous section. Mills and Sarikakis also believed that mass surveillance has increased the vulnerability of journalists who abandoned traditional “watchdog” journalism and worked with hacktivists to disclose how national security laws increased mass surveillance of civilian and civil parties. This non-traditional journalistic role has exposed female journalists to higher risks of being surveilled, which indicates how their vulnerability is affected by the legislative context of national security laws in western democracies.

Likewise, censorship and internet control in limited democracies, repressive societies, and authoritarian regimes, and also challenge the protection of journalists' digital safety (Mills 2019). Countries including China, Russia, and Turkey, have outlawed some prevalent digital safety tools, such as the Virtual Private Network (VPN), which increases the vulnerability of journalists (Henrichsen, Betz, and Lisosky 2015; ProtonVPN). Journalists in Hong Kong also reported that they withdrew some stories under the pressure of Chinese Public Security Bureau (Tsui and Lee 2019).

In sum, both social and legislative contexts could compromise journalists' vulnerability to digital surveillance and malware attacks. Whereas the implications of social-cultural contexts are more subtle, legislative contexts exert a direct impact on journalists’ vulnerability.

2.4. Journalists’ Strategies for Digital Safety

Given the intense digital surveillance and malware attacks they face, journalists have developed diversified approaches regarding their digital safety. Tsui and Lee (2019) have developed their theories based on the following previous study, and categorized journalists’ security as opportunity. Details and limitations of each strategy will be provided in the following paragraphs strategies of digital safety into three types: security by obscurity, security by obfuscation and security as opportunity. Details and limitations of each strategy will be provided in the following paragraphs.
2.4.1. Security by obscurity

The concept of “security by obscurity”, also called “security through obscurity”, originally comes from a cybersecurity term referring to a belief that nobody will discover security holes, and therefore fixing security holes are unnecessary (The Jargon File; Mercuri and Neumann 2003). McGregor and Watkins adapt the term “security by obscurity” to describe a prevalent strategy amongst journalists that they will only secure their data when working on sensitive topics relevant to state actors (McGregor and Watkins 2016).

Tsui and Lee (2019) have followed previous studies by expanding the definition of “security by obscurity”. Journalists covering non-sensitive topics are indifferent to digital safety. In another study done by Tsui (2019), some journalists and their editors in local newspapers regarded digital protective measures as unnecessary, because they believed their local news agencies as insignificant (Tsui 2019). This finding parallels the result of the Digital Rights Foundation’s study on female journalists in Pakistan (Digital Rights Foundations 2017). In Waters’ (2018) study some participants thought their topics were not important enough to cause the attention by the state, and therefore they did not need to secure their data (Water 2018). Meanwhile, journalists tend to censor their news content to achieve the goal of “security by obscurity” strategy. Because of their beliefs that non-sensitive topics would protect them from digital surveillance, they omitted topics relevant to politics in their news reports, so as to avoid state surveillance.

However, the “security by obscurity” strategy cannot protect journalists’ digital safety. First, avoiding some certain topics would not reduce digital surveillance of journalists, since mass surveillance is targeting everyone (Mills and Sarikakis 2016; Waters 2018). Second, with the advancement of technology and a reduction of the costs to conduct digital surveillance and
malware attacks (Henrichsen, Betz, and Lisosky 2015), journalists need to take advanced protective measures.

2.4.2. Security by obfuscation

Obfuscation is another commonly used strategy in cryptography. The goal of this strategy is to create obstacles to unverified access of accounts and therefore reduce risks of forced entry. For instance, internet users set up encrypt passwords with security keys and encryption algorithms, and therefore increase difficulties for others to access their accounts (Boyen, Chen, and ProvSec 2011; Eclipse Foundation).

Based on the cryptography concept, Tsui and Lee developed the term “security by obfuscation” to describe another prevalent digital safety strategy amongst. Journalists who have adopted this strategy prefer the use of low-end techniques to secure their digital communication, such as by speaking in code words or misspelling words (Tsui and Lee 2019). They also use offline communication and storage like face meetings and writing down, printing, and/or copying confidential information onto encrypted disks. Some of them will meet in a noisy area or put their phone aside or use laptops disconnected from the Internet to reduce the chance of being surveilled on the phone. (Milosavljević, Prodnik, and Kučić 2015; Waters 2010).

This strategy has some limitations. Originating from an old tradition of “do not discuss the sensitive issues over the phone” prevalent 20 years ago (Milosavljević, Prodnik, and Kučić 2015), this strategy is out-of-date and low technical for journalists to defend against the evolving surveillance technology.

2.4.3. Security by opportunity

Tsui and Lee (2019) use “security by opportunity” to describe a strategy of journalists who consider the use of digital protective measures as a good opportunity for their career. They are aware of the importance of protecting their sources, and therefore using digital safety is part of
their job responsibility to protect their career reputation. They also recognize that the use of digital protective measures help them to exceed limits of self-censorship, as a result of digital surveillance against and malware attacks on them, and cover topics relevant to sensitive and contentious issues, such as politics and national security. Journalists who adopt this strategy use digital protection frequently, and they are willing to continually invest their time and money in using digital safety tools.

Journalists with the “security as opportunity” strategies are willing to learn and apply high-tech measures to protect their digital safety. These high-tech measures include “the use of encrypted chat apps and VPNs to circumvent censorship and to preserve a level of privacy” (Tsui and Lee 2019: 11). According to Waters (2018), some newsrooms require journalists to include the following digital safety tools in their daily workflows: (1) Encrypted email and messaging services, such as Protonmail and Signal, (2) Pretty Good Program (hereafter “PGP”) that provides cryptographic privacy and authentication for data communication for signing, encrypting, and decrypting texts, e-mails, files, directories, and disks, VPN secure their internet connections, and SecureDrop for securing the cloud storage (Henrichsen, Betz, and Lisosky 2015). These tools helps journalists and newsrooms exceed the limits caused by digital surveillance and creates more opportunity for them to cover diversified topics. Therefore, it is beneficial for journalists’ career development as well as newsrooms’ reputations for caring about the safety of its employees (Tsui and Lee 2019).

However, this strategy carries huge costs of time and money. The evolving nature of technologies lowers the barrier and costs of digital surveillance, and therefore, it raises the bar of journalists’ digital safety protection. Journalists have to spend money on the latest digital protection equipments (Henrichsen, Betz, and Lisosky 2015). Even if some digital protection
tools are affordable for individual journalists, still it requires a learning curve for them to use. Some reporters also complained that the use of digital protection was time-consuming in their daily work (Waters 2018; Mills and Sarikakis 2016). For instance, some investigative reporters in Eastern Europe often have a huge volume of digital communication to be encrypted, which is not possible to encrypt the data in the short amount of time (Milosavljević, Prodnik, and Kučić, 2015). Based on these reasons, newsrooms need to provide easy access for their journalists to digital protection, such as company VPN to use their daily work or technical support to install the digital safety tools. This will be explained more in the organizational support section.

2.5. Existing practices by other stakeholders

By reviewing the existing strategies taken by journalists in the previous section, I discover the protection of journalists also requires efforts from various stakeholders, particularly their newsrooms, journalist communities and policy makers. This section will review the existing practices established by each of these stakeholders. Starting from organizational support offered by newsrooms, I will also review the existing practices across global journalist communities, such as normative frameworks and toolkits for journalists to protect their digital safety. Next, I will talk about the international and regional efforts to establish principles to define and guarantee journalists’ digital safety. However, each of these existing practices have their own limitations, which will be provided with each practice’s section.

2.5.1. Organizational efforts of newsroom

There are various newsrooms’ efforts in regard to protecting their journalists from digital surveillance and malware attacks. Some newsrooms require the use of digital safety in journalists’ daily work, such as a specific workflow of securing their sources, internet connections, emails and SMS messages, and hard drives. For example, some newsrooms provided company VPNs for their staff and required them to use it on a regular basis (Waters
In addition to providing certain tools, some newsrooms have established their special departments to offer skills training and technical support for journalists to secure their data (Digital Rights Foundation 2017).

These organizational efforts are heavily reliant on newsrooms’ financial capabilities or their legacy of creating a secure professional environment. For example, a local branch of an international news company, which is better funded and experienced, is more likely to offer cybersecurity training than a local small newspaper (Digital Rights Foundation 2017). Therefore, newsrooms with limited access to resources need more support from the international journalist communities to protect their employees’ digital safety.

2.5.2 Efforts across journalist communities

Journalist communities, including global journalists’ networks, nonprofit organizations and research institutions, have taken efforts to protect the digital safety of global journalists. Some of the efforts have contributed to the study and insights of journalists’ digital safety, the establishment of global normative frameworks, and training or toolkits systems for global journalists.

**The United Nations framework**

The United Nations and The United Nations Educational, Scientific and Cultural Organization (UNESCO) has formulated a plan to establish the principles for protecting journalists’ digital safety in 2017. This plan is called The UN Plan of Action on the Safety of Journalists and the Issue of Impunity (the UN Plan).

The UN plan specifies the responsibility of news organizations to “improve digital safety and develop strategies to address online violence and harassment of journalists” (OHCHR 2017: 3.3.22). To achieve this goal, news organizations need to take the following measures:
● Newsrooms should cooperate with internet companies to ensure the protection of journalist’s data when they are using the internet service.

● Newsrooms should have immediate response to online harassment and abuse for journalists, particularly female journalists.

● Newsrooms should have effective safety protocols to ensure journalists’ digital safety as well as legal support for journalists.

● Newsrooms may consider establishing digital safety protection workflows.

**Journalist safety principle**

In 2015, “The Freelance Journalist Safety Principle” was launched and endorsed by major news companies and journalism organizations across the globe to establish worldwide freelance protection standards. The standards emphasized that journalists should “secure mobile and Internet communications from intrusion and tracking” (Freelance Journalist Safety Principles 2015). Similarly, the “International Declaration on the Protection of Journalists for Nations and News Organizations” suggests that news agencies should provide digital training for their news staff to increase safety awareness and reduce risks (The International Press Institute 2016).

**Digital safety toolkit and training**

The Committee to Protect Journalists (CPJ) has produced a digital safety kit for journalists to secure “their accounts, devices, communications and online activity” (Committee to Protect Journalists 2019). Some of the recommended measures are listed as follows.

- Journalists should have a full assessment of their digital security. The assessment includes checking password security and accounts’ privacy settings, examining the security of data stored on these accounts and their digital devices, and evaluating the potential consequence of data leaks. These accounts can be emails, social media and
messaging services. They should also remove sensitive data and back up their data on a regular basis.

- Journalists should be alerted to suspicious emails or messages to avoid phishing attacks. Suspicious emails or messages often contain links or attachments that “urge you to do something quickly or appear to be offering you something that appears to be good to be true”. To avoid being tricked by these phishing links or attachments, journalists may verify the legitimacy of sender's accounts, content details, such as spelling, grammar, and layout, and preview these attachments or links before clicking in or downloading.

- Journalists should update operating systems regularly to fix security loopholes and defend against latest malware.

- Journalists should use complex passwords to lock their devices and utilize encryption tools for hard drives and storage.

- Journalists should also consider using VPN to secure Internet connection, confirm websites’ authenticity by checking their web address with tools.

Other organizations, such as UNESCO (2007), Dart Center for Journalism & Trauma Research Lab at The University of Tulsa (2017) and Deutsche Welle (DW.com), have also provided seminars, training modules and consultation for journalists to secure their sources and data.

As referenced above, journalist communities have been making efforts to support journalists and their newsrooms. Yet their normative frameworks are not legally binding, so they provide no mandatory requirements for news organizations to enforce. The digital safety toolkits they offer mostly rely on journalists’ individual efforts to learn and apply the skills rather than the organizational efforts from newsrooms. They are also somewhat outdated. For example, the UN
plan is based on two studies prior to 2017, “Building digital safety for journalism: a survey of selected issues” (Henrichsen, Betz, and Lisosky 2015) and “Protecting Sources In the Digital Age” (Poseti 2017). These toolkits may not be effective enough to shield journalists from digital surveillance and malware attacks. Due to the advancement of surveillance technology and the reduced costs of producing malware, the number of digital surveillance and malware attacks are surging globally (Henrichsen, Betz, and Lisosky 2015). For instance, the AI surveillance technologies have been applied in 176 countries since 2017 (Schwartz 2019). With regard to the surge number of digital threats, journalists need advanced measures to secure their data. In particular, they need guidance to conceal their identity information, protect their work data, and avoid being prosecuted in different political and cultural contexts. However, due to the nonprofit nature of these organizations, they may have limited access to advanced technology and sufficient funding to support journalists compared to commercial malware developers.

2.5.3. Efforts of policy and law makers

Some legal frameworks have been established to protect journalists from the threats and risks that are caused by digital surveillance and malware attacks.

The United Nations Article 19

The UN has enacted Article 19 to establish a legal framework to ensure journalists’ rights to fulfil their jobs independently, including being free from the surveillance under national security laws, stop the digital surveillance of journalists’ devices, and abolish legal frameworks that “arbitrarily arrest or detain journalists, and release those in detention” (Article 19 2017: 16).

Regional legal frameworks

Under the framework of the UN Article 19, regional human rights institutions in Europe and Central Asia (OSCE), the Americas (OAS), and Africa (ACHPR), have established mechanisms to enforce the UN legal frameworks and address the issue of journalists’ digital safety.
The European Union (EU) has also established a legal framework to ensure the protection of journalists’ safety, including digital safety. This framework is based on the principle of protecting freedom of speech, that was established by The European Court of Human Rights (ECtHR). It reiterates the importance of protecting journalists’ sources, their rights to access information freely, and their freedom to “hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers” (European Convention on Human Rights:10.1). Besides, the European Court has enacted laws of data protection (Council of Europe n.d. a) and founded a special committee to address cybercrime (Council of Europe n.d. b). These two measures provide protection for the data privacy and cybersecurity of European journalists.

The EU legal framework recognizes the evolving nature of journalism as a result of new media in the digital age, and therefore includes non-traditional journalists who “who contribute to public debate and who perform journalistic activities or fulfil public watchdog functions” (Council of Europe 2016:4) in the protection. Second, it encourages newsroom and civil society to establish of “early-warning and rapid-response mechanisms, such as hotlines, online platforms or 24-hour emergency contact points “ (Council of Europe 2016: I (10), to ensure that journalists can have immediate access to protection when they are threatened by safety risks, including digital surveillance and malware attacks. This is parallel to the guidelines of the UN framework.

Although these frameworks aim to provide a legal ground for protecting journalists’ digital safety, they are not legally binding. Newsrooms are not legally obligated to provide organizational support, and journalists will not receive any legal remedy once their digital safety is compromised, such as when their devices are attacked, or their newsrooms refuse to provide
cybersecurity training. In addition, regions such as Oceania, do not have a mechanism to deal with the issue of journalists’ digital safety.

2.6. Chapter Summary
In this section, I will present the key takeaways from the existing literature as well as providing a glossary of technical terms that appear in the existing literature.

Here are the key takeaways from the existing literature review:

● Digital surveillance and malware attacks have posed severe threats to journalists' personal safety. As a result, it has caused self-censorship of journalists and newsrooms, which results in breaches of freedom of speech. The breaches of freedom of speech will compound the situation of digital surveillance, and therefore, journalism’s “watchdog” role could be limited, which triggers the erosion of democracy.

● Some examples, such as the murder of Jamel Koshosggi, indicated that digital surveillance and malware attacks often intersect with each other, though it is not explicitly articulated in the existing literature. Malware attacks can serve as a means of digital surveillance of journalists, and digital surveillance can be a facilitator of malware attacks against journalists.

● Journalists have different strategies for addressing digital threats. “Security by obscurity” is often used by journalists who believe that no measures can shield them from digital surveillance and malware attacks. In contrast, journalists with the other two strategies, “security by obfuscation” and “security by opportunity,” take measures to protect their digital safety. The major differences between these two strategies are whether journalists regard the use of digital protection positively or their measures involve advanced technologies.
Newsrooms, journalist communities, and policy makers are stakeholders to enforce the protection of journalists' digital safety. They have established some existing practices of training modules, digital safety toolkits and normative frameworks. However, they should update training modules and digital safety toolkits with advanced technology. They may also enforce the normative and legal frameworks by legal means. This requires a collaboration between newsrooms, journalist communities, and law and policy makers.
Chapter 3. Methodology, Hypothesis, and Analysis

In this chapter, I will discuss my methodology, which is a quantitative approach to conduct a secondary data analysis. This methodology is legitimate, as the survey was conducted by a professional team and the collected data contains relevant questions for my research. I will also explain my seven hypotheses, derived from my three research questions, and demonstrate their legitimacy by paralleling the findings from my literature review. Later, I am going to examine my hypotheses with the dataset. In particular, I will conduct crosstab analysis to examine the relationships among different variables. These variables are: journalists’ frequency of use digital protection, whether journalists believed cybersecurity is the most helpful, whether newsroom offered cybersecurity training, the news content they covered most often, the media formats they used, journalists’ newsroom positions, journalists’ technical skills before they got hired by the current newsrooms, the region in which journalists work, journalists’ gender, and newsroom type.

My major finding is that over a majority of journalists did not secure their data. This finding is worrisome since it may compound their vulnerability to digital surveillance and attacks. In addition, my findings also prove my hypothesis that journalists’ use of digital protection are related to the news content they covered most often, the media formats they used, their newsrooms positions, their technical skills before they got hired by the current newsrooms, the region in which journalists work, and their gender. Moreover, my findings also show that very few newsrooms offered cybersecurity training for their news staff, and among them online-only or digital-only newsrooms are most likely to provide organization training for journalists to increase their awareness and secure their data.

3.1. Research Questions

In this study, my research questions are:

RQ1: What do journalists do to ensure their digital safety?
RQ2: What influences journalists’ use of digital protection?

RQ3: What challenges do journalists face in their efforts to ensure their digital safety?

I used a quantitative approach to explore my research questions. I used the 2019 State of Technology in Global Newsrooms survey as my data source and conducted data analyses based on the survey data. I examined seven hypotheses and identified the relationship among different variables: the news content they covered most often, the media formats they used, their newsroom positions, their technical skills before they were hired by the current newsrooms, the regions in which journalists work, and their gender. In the following section, my methodology and my analyses will be further presented.

3.2. Methodology

I took a quantitative analysis approach to explore my research questions. In this section, I am going to explain my quantitative method and the rationale to use this method.

3.2.1. This dataset

I selected the data from the 2019 State of Technology in Global Newsrooms survey as my major source of data. This survey has collected responses from 3,600 journalists and 500 newsroom managers in 149 countries. Dr. Diana Owen, Professor at the Georgetown Communication, Culture and Technology Program, in conjunction with the International Center for Journalists (ICFJ), conducted the survey. ICFJ has been working with more than 140,000 journalists and newsroom managers from 180 countries over the past 35 years, which proves their reputation as a professional team to conduct research relevant to journalism (International Center for Journalists 2019).

3.2.2. Rationale

The dataset of the 2019 State of Technology in Global Newsrooms survey is an appropriate source for the following two reasons.
First, this survey includes questions regarding how journalists ensure their digital safety and their use of using digital protection. Journalists were inquired about their frequency of using each digital protection, including secure messaging, encrypted emails, secure video or audio calls, and company or personal VPNs. The frequency of using the digital protection is categorized by daily, weekly, monthly, and never or rarely. The frequency of using the digital protection is categorized by daily, weekly, monthly, and never or rarely. For example, journalists may use secure messaging on a daily basis, and check their secure email 2-3 times a week. The difference of frequency could reflect their attitude towards digital safety.

In addition, this dataset is also relevant to my research questions in the following ways:

- The dataset provides background information: participants were asked about their regions and gender. This information provides a gender and regional division of journalists’ use of digital protection, which could result from social or legislative contexts varying based on regions.

- The dataset provides context of journalists’ work in their newsrooms: the media format used in their newsrooms, types of their newsrooms, their newsroom positions, and their content areas that they covered most often.

- This dataset provides information on journalists’ technical skills. Journalists were asked about whether they were hired because they have one or more following skills: (1) using cybersecurity, (2) researching or distributing stories with social media, (3) working with data journalism, and (4) using digital video, audio or photo tools.

  - The dataset investigates whether journalists’ newsrooms provided cybersecurity training: newsroom managers were asked about whether and in what formats their newsrooms offered cybersecurity training. In addition, Journalists were also asked about whether
cybersecurity training is the most helpful for them, as well as what training formats were the most effective.

Second, this dataset contains 3,060 responses of from 3,060 journalists in 149 countries. It gives me broad international representativeness of the desired population of respondents because of the large number of journalists participating in the study (International Center for Journalists 2019).

3.3. Hypothesis and Justification
I derived the following hypotheses from my research questions. I predicted that journalists’ use of digital protection is influenced by different factors. Hence:

**H1: Journalists’ use of digital protection is closely related to their news content.**

**Journalists who cover sensitive beats are more likely to use digital protection frequently.**

**Journalists who cover local news are less likely to secure their data.**

This hypothesis aligns with the literature review. Journalists who covered sensitive topics reported that they were more vulnerable to digital surveillance. These certain sensitive topics include national security, religion, gender issues, government corruption, human rights violations, police policies, military, and foreign ministry affairs (Mills 2019; Digital Rights Foundation 2017; Tsui and Lee 2019). Investigative reporters are also more likely to be surveilled or attacked in the digital space. By contrast, their counterparts who covered hyper local news, or only relied on press releases as their main sources, regard their job as unimportant, and therefore, they believed digital protection was unnecessary for them (Milosavljević, Prodnik, and Kučić 2015; Tsui and Lee 2019).

**H2: Media formats influence journalists’ frequency of using digital protection. In general, journalists working with online media are most likely to use digital protection frequently.** Among legacy news outlets, printed newspaper and television journalists are
more likely to protect their digital safety compared with their counterparts in radio or print magazines.

This hypothesis parallels the literature review. The data of online journalists is oftentimes collected by law enforcement and used to press charges against them, and as a result, the majority of global imprisoned journalists (60%) worked for online media (Committee to Protect Journalists 2019). This may indicate that online media journalists are more likely to protect their digital safety because they are exposed to high risks of being surveilled. In addition to online media, journalists working for printed newspapers and televisions reported they are more subject to digital surveillance conducted by social actors compared to their peers in other legacy news outlets (Digital Rights Foundation 2017).

**H3: Journalists’ newsroom positions influence the frequency of their use of digital protection. Full-time and investigative reporters are more likely to secure their data more frequently than their editors and freelance peers.**

This is based on the finding of Digital Rights Foundation (2017), which is presented in the literature review. Compared with their editorial peers, journalists are more vulnerable because they need to be in the field and have direct contact with sources. Meanwhile, freelance journalists are lacking in organizational support for digital safety, and therefore they are more likely to suffer digital surveillance and attacks.

**H4: Journalists’ technical skills influence their frequency of using digital protection. In particular, journalists with cybersecurity skills use digital protection more frequently than their peers.**

This hypothesis is based on the Water’s finding (2018) that journalists who have a solid understanding of technology tend to have a higher awareness of digital safety. Journalists
who reported that they were familiar with computer skills tended to have a higher awareness of the consequences of digital surveillance and therefore would secure their data.

**H5: The region in which journalists work influences their frequency of using digital protection.**

This hypothesis aligns with some of my findings from the literature review. According to the existing literature, journalists’ vulnerability to digital surveillance may vary across different regions, including democratic and repressive regimes in Europe, North America, Asia and Africa. For instance, Mills (2019) claimed that journalists in democratic countries, such as western democracies, have less concern about surveillance. In contrast, digital surveillance was more severe in limited democracies, repressive societies, and authoritarian regimes, such as Hungary, Poland, Egypt, and Turkey. Therefore, I anticipated that journalists in western democracies used digital protection at the lowest rate. The existing literature does not specify journalists in which region use digital protection most or least, so the examination of H5 is helpful to identify this information.

**H6: Female journalists are less likely to use digital protection compared to their male peers.**

This hypothesis is based on the finding from the existing literature that female journalists are subject to digital surveillance (Henrichsen, Betz, and Lisosky 2015; Digital Rights Foundation 2017). Due to their topics, gender stereotypes against them. Often they are lacking in protective resources, such as cybersecurity training (Westcott 2019) and a mechanism to report digital attacks they were confronted with (Digital Rights Foundation 2017). Thus, I anticipated that female journalists use digital protection less than their male counterparts, which may be one reason for their greater vulnerabilities.
H7: Journalists’ access to cybersecurity training varies based on types of their newsrooms.

This hypothesis parallels some of the findings from my literature review. In particular, Water (2018), Tsui and Lee (2019) and Digital Rights Foundation (2017) discovered that certain types of newsrooms were likely to include digital safety tools in their regular workflows. These newsrooms include newsrooms that cover sensitive issues, introduced in the previous section discussing the legitimacy of H1, conspicuous areas such as national and international news, or a local branch of international news organizations. Therefore, I predicted that types of journalists’ newsrooms are related to their access to cybersecurity training offered by their newsroom.

3.4. Analytics and Finding

After checking to ensure the data are valid, a series of crosstabs analyses were performed to test H1-H7. My analyses are presented as follows.

3.4.1. News content variable (H1)

H1 predicts journalists’ beats influence their use of digital protection. The hypothesis was tested by two crosstabs, and it is supported by the following analyses:

Journalists who covered sensitive and conspicuous topics are more aware of the importance of securing their data, and they do use digital protection more frequently compared to their peers. 20.7% of investigative reporters used digital protection daily compared to 18.4% of crime reporters, 16.3% of political reporters, and 16.6% of economy reporters. This indicates that journalists who often cover investigative reports, which are considered sensitive topics, used digital safety more frequently than their counterparts. This also shows that journalists’ lack of digital protection is alarming. Investigative journalists had the biggest number to secure their data, yet most of them were less likely to take protective measures. Journalists who covered politics and crime, which were also considered as sensitive and
contentious topics, are also less likely to use any digital protection. Overall, a majority of journalists of each beat rarely or never used digital protection (over 60% of political reporters and economy reporters, over 50% of investigative reporters, and nearly 60% of crime reporters). The relationship between digital protection and news types is statistically significant at $p \leq .00$.

<table>
<thead>
<tr>
<th>% within beats</th>
<th>Daily</th>
<th>Weekly</th>
<th>Monthly</th>
<th>Rarely/never</th>
</tr>
</thead>
<tbody>
<tr>
<td>Politics</td>
<td>16.3%</td>
<td>8.2%</td>
<td>11.6%</td>
<td>63.9%</td>
</tr>
<tr>
<td>Investigative reports</td>
<td>20.7%</td>
<td>11.7%</td>
<td>13.5%</td>
<td>54.2%</td>
</tr>
<tr>
<td>Crime</td>
<td>18.4%</td>
<td>9.9%</td>
<td>12.2%</td>
<td>59.6%</td>
</tr>
<tr>
<td>The economy</td>
<td>16.6%</td>
<td>9.1%</td>
<td>11.5%</td>
<td>62.8%</td>
</tr>
<tr>
<td>Total</td>
<td>14.9%</td>
<td>8.5%</td>
<td>11.5%</td>
<td>65.1%</td>
</tr>
</tbody>
</table>

Journalists who regarded cybersecurity training useful occupied less than 30% of the total number of journalists covering hyper local news and local news respectively (hyper local news: 26.3%; local news: 28.7%). The relationship between news types and cybersecurity training is statistically significant at $p \leq .003$.

<table>
<thead>
<tr>
<th>% within beats</th>
<th>Daily</th>
<th>Weekly</th>
<th>Monthly</th>
<th>Rarely/never</th>
</tr>
</thead>
<tbody>
<tr>
<td>Traditional formats</td>
<td>14.7%</td>
<td>5.7%</td>
<td>8.0%</td>
<td>71.5%</td>
</tr>
<tr>
<td>Online or digital formats</td>
<td>16.7%</td>
<td>11.5%</td>
<td>15.0%</td>
<td>56.8%</td>
</tr>
<tr>
<td>Print newspaper</td>
<td>13.4%</td>
<td>6.7%</td>
<td>7.7%</td>
<td>72.1%</td>
</tr>
<tr>
<td>Television</td>
<td>15.3%</td>
<td>7.2%</td>
<td>7.5%</td>
<td>70.0%</td>
</tr>
<tr>
<td>Print magazine</td>
<td>3.0%</td>
<td>4.5%</td>
<td>14.9%</td>
<td>77.6%</td>
</tr>
<tr>
<td>Radio</td>
<td>16.9%</td>
<td>7.9%</td>
<td>12.2%</td>
<td>63.0%</td>
</tr>
<tr>
<td>Website</td>
<td>15.8%</td>
<td>10.5%</td>
<td>14.5%</td>
<td>59.3%</td>
</tr>
<tr>
<td>News App</td>
<td>17.6%</td>
<td>14.7%</td>
<td>14.7%</td>
<td>52.9%</td>
</tr>
<tr>
<td>Podcast</td>
<td>0.0%</td>
<td>26.7%</td>
<td>6.7%</td>
<td>66.7%</td>
</tr>
<tr>
<td>Email newsletter</td>
<td>20.0%</td>
<td>6.7%</td>
<td>15.6%</td>
<td>57.8%</td>
</tr>
<tr>
<td>Social media</td>
<td>18.8%</td>
<td>6.3%</td>
<td>9.4%</td>
<td>65.6%</td>
</tr>
</tbody>
</table>

3.4.3. Position variable (H3)

H3 predicts that journalists’ newsroom positions in their newsrooms influence their frequency of using digital protection. I conducted one crosstab to test the relationship of these two variables. The analysis supports H2 by providing the following information:
23.4% of investigative reporters used digital protection daily, more than 10% higher compared to 11.9% of beat reporters, 12.5% news reporters, and 19% of their editorial peers.

In addition, only 11.8% of freelance journalists secured their data daily. The relationship between journalists’ positions and digital protection is statistically significant at $p \leq .00$.

<table>
<thead>
<tr>
<th>% within positions</th>
<th>Helpful</th>
<th>Not helpful</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hyper local (e.g. community news)</td>
<td>26.3%</td>
<td>73.7%</td>
</tr>
<tr>
<td>Local (e.g. town or city news)</td>
<td>28.7%</td>
<td>71.3%</td>
</tr>
<tr>
<td>National news</td>
<td>33.8%</td>
<td>66.2%</td>
</tr>
<tr>
<td>Regional news</td>
<td>31.6%</td>
<td>68.4%</td>
</tr>
<tr>
<td>International news</td>
<td>24.0%</td>
<td>76.0%</td>
</tr>
<tr>
<td>Some combination of local, regional, national, and international news</td>
<td>37.2%</td>
<td>62.8%</td>
</tr>
</tbody>
</table>

### 3.4.2. Media format variable (H2)

H2 expects that media formats and journalists’ newsroom influence their frequency of using digital protection. To test this hypothesis, I used one crosstab to examine the variable relationship. The analysis supports H2 by providing the following information:

16.7% of journalists working with online or digital formats used digital protection daily, 2 percentage points higher than their counterparts working with traditional formats. 13.4% and 15.3% of journalists in print newspapers and televisions used digital protection daily respectively, about 5 times higher than their radio counterparts. The relationship between media formats and digital protection is statistically significant at $p \leq .00$.

<table>
<thead>
<tr>
<th>% within beats</th>
<th>Daily</th>
<th>Weekly</th>
<th>Monthly</th>
<th>Rarely/never</th>
</tr>
</thead>
<tbody>
<tr>
<td>Traditional formats</td>
<td>14.7%</td>
<td>5.7%</td>
<td>8.0%</td>
<td>71.5%</td>
</tr>
<tr>
<td>Online or digital formats</td>
<td>16.7%</td>
<td>11.5%</td>
<td>15.0%</td>
<td>56.8%</td>
</tr>
<tr>
<td>Print newspaper</td>
<td>13.4%</td>
<td>6.7%</td>
<td>7.7%</td>
<td>72.1%</td>
</tr>
<tr>
<td>Television</td>
<td>15.3%</td>
<td>7.2%</td>
<td>7.5%</td>
<td>70.0%</td>
</tr>
<tr>
<td>Print magazine</td>
<td>3.0%</td>
<td>4.5%</td>
<td>14.9%</td>
<td>77.6%</td>
</tr>
<tr>
<td>Radio</td>
<td>16.9%</td>
<td>7.9%</td>
<td>12.2%</td>
<td>63.0%</td>
</tr>
<tr>
<td>Website</td>
<td>15.8%</td>
<td>10.5%</td>
<td>14.5%</td>
<td>59.3%</td>
</tr>
<tr>
<td>News App</td>
<td>17.6%</td>
<td>14.7%</td>
<td>14.7%</td>
<td>52.9%</td>
</tr>
<tr>
<td>Podcast</td>
<td>0.0%</td>
<td>26.7%</td>
<td>6.7%</td>
<td>66.7%</td>
</tr>
<tr>
<td>Email newsletter</td>
<td>20.0%</td>
<td>6.7%</td>
<td>15.6%</td>
<td>57.8%</td>
</tr>
<tr>
<td>Social media</td>
<td>18.8%</td>
<td>6.3%</td>
<td>9.4%</td>
<td>65.6%</td>
</tr>
</tbody>
</table>
3.4.3. Position variable (H3)

H3 predicts that journalists’ newsroom positions in their newsrooms influence their frequency of using digital protection. I conducted one crosstab to test the relationship of these two variables. The analysis supports H2 by providing the following information:

23.4% of investigative reporters used digital protection daily, more than 10% higher compared to 11.9% of beat reporters, 12.5% news reporters, and 19% of their editorial peers. In addition, only 11.8% of freelance journalists secured their data daily. The relationship between journalists’ positions and digital protection is statistically significant at \( p \leq 0.00 \).

<table>
<thead>
<tr>
<th>% within positions</th>
<th>Daily</th>
<th>Weekly</th>
<th>Monthly</th>
<th>Rarely/never</th>
</tr>
</thead>
<tbody>
<tr>
<td>Investigative Reporter</td>
<td>23.4%</td>
<td>14.1%</td>
<td>12.5%</td>
<td>50.0%</td>
</tr>
<tr>
<td>Beat Reporter</td>
<td>11.9%</td>
<td>5.8%</td>
<td>6.1%</td>
<td>76.3%</td>
</tr>
<tr>
<td>News Reporter</td>
<td>12.5%</td>
<td>7.4%</td>
<td>10.2%</td>
<td>69.9%</td>
</tr>
<tr>
<td>Editors (editor writers and editorial leadership)</td>
<td>19%</td>
<td>7.9%</td>
<td>14.2%</td>
<td>58.3%</td>
</tr>
<tr>
<td>Freelance Journalist</td>
<td>11.8%</td>
<td>4.6%</td>
<td>13.2%</td>
<td>70.4%</td>
</tr>
</tbody>
</table>

3.4.4. Technical skill (H4)

H4 predicts that journalists’ technical skills influence their frequency of using digital protection. This hypothesis was tested by one crosstab and is supported by the analysis. 17.1% of journalists having two or more skills used digital protection daily, nearly twice as much as 8.9% of journalists having no technical skills. In particular, 38.7% of journalists with cybersecurity skills used digital protection daily, compared to 20% of journalists with data journalism skills, 16.6% of journalists with skills in digital video, audio or photo tools, and 16.3% of journalists with social media skills to research or distribute stories. Moreover, 80% of journalists having no technical skills never or rarely used digital protection, 4 times as much as 17.8% of journalists having digital protection skills. The relationship between technical skills and digital protection is statistically significant at \( p \leq 0.00 \).
Table 6. Technical Skills and Frequency of Using Digital Protection

<table>
<thead>
<tr>
<th>% within skills</th>
<th>Daily</th>
<th>Weekly</th>
<th>Monthly</th>
<th>Rarely/never</th>
</tr>
</thead>
<tbody>
<tr>
<td>No skills</td>
<td>8.9%</td>
<td>4.0%</td>
<td>6.4%</td>
<td>80.7%</td>
</tr>
<tr>
<td>Have 1 skills</td>
<td>14.9%</td>
<td>6.9%</td>
<td>11.6%</td>
<td>66.6%</td>
</tr>
<tr>
<td>Have 2 or more skills</td>
<td>17.1%</td>
<td>11.0%</td>
<td>13.2%</td>
<td>58.8%</td>
</tr>
<tr>
<td>Cybersecurity</td>
<td>38.7%</td>
<td>25.2%</td>
<td>18.4%</td>
<td>17.8%</td>
</tr>
<tr>
<td>Data journalism</td>
<td>20.0%</td>
<td>10.6%</td>
<td>14.1%</td>
<td>20.0%</td>
</tr>
<tr>
<td>Digital video, audio or photo tools</td>
<td>16.6%</td>
<td>10.5%</td>
<td>11.8%</td>
<td>61.2%</td>
</tr>
<tr>
<td>Use social media to research or distribute stories</td>
<td>16.3%</td>
<td>9.8%</td>
<td>12.6%</td>
<td>61.3%</td>
</tr>
</tbody>
</table>

3.4.5. Region (H5)

H5 expects that the regions where journalists are located influence their frequency of using digital protection. This hypothesis was examined by one crosstab and is supported by the following analysis: 30.5% of journalists in the South Asia region and 18.5% of journalists in East and Southeast Asia used digital safety frequently, compared to 5.5% of journalists in Europe and 12.5% of journalists in North America. Meanwhile, 17.1% of journalists in Sub-Saharan Africa used digital protection daily, three times more than 5.5% of their European counterparts. Additionally, the majority of journalists in Latin America/Caribbean, Middle East/North Africa, Europe, and North America never or rarely used digital protection, occupying over 70% of the journalist numbers in these regions. This indicates that journalists who use digital protection daily are more numerous in developing regions, especially in Asia, than in developed regions such as North America and Europe, which are also western democracies. The relationship between technical skills and digital protection is statistically significant at $p \leq 0.00$.

Table 7. Region and Frequency of Using Digital Protection

<table>
<thead>
<tr>
<th>% within region</th>
<th>Daily</th>
<th>Weekly</th>
<th>Monthly</th>
<th>Rarely/Never</th>
</tr>
</thead>
<tbody>
<tr>
<td>Latin America/Caribbean</td>
<td>11.0%</td>
<td>6.1%</td>
<td>9.5%</td>
<td>73.4%</td>
</tr>
<tr>
<td>Middle East/North Africa</td>
<td>8.0%</td>
<td>6.3%</td>
<td>9.2%</td>
<td>76.5%</td>
</tr>
<tr>
<td>Sub-Saharan Africa</td>
<td>17.1%</td>
<td>10.0%</td>
<td>10.3%</td>
<td>62.6%</td>
</tr>
<tr>
<td>East and Southeast Asia</td>
<td>18.5%</td>
<td>13.5%</td>
<td>13.9%</td>
<td>54.1%</td>
</tr>
<tr>
<td>South Asia</td>
<td>30.5%</td>
<td>9.5%</td>
<td>10.0%</td>
<td>50.0%</td>
</tr>
<tr>
<td>Europe</td>
<td>5.5%</td>
<td>6.6%</td>
<td>16.5%</td>
<td>71.4%</td>
</tr>
<tr>
<td>North America</td>
<td>12.5%</td>
<td>8.8%</td>
<td>6.3%</td>
<td>72.5%</td>
</tr>
</tbody>
</table>
3.4.6. Gender (H6)

H6 predicts that journalists’ genders influence their frequency of using digital protection.

This hypothesis was examined by one crosstab and is supported by the following analysis:

11.6% of female journalists used digital protection daily, more than 5% less compared to 16.9% of their male peers. In addition, 71.8% of female journalists rarely or never used digital protection, 10 percentage points more than their male counterparts. The relationship between technical skills and digital protection is statistically significant at p≤.00.

<table>
<thead>
<tr>
<th>% within gender</th>
<th>Daily</th>
<th>Weekly</th>
<th>Monthly</th>
<th>Rarely/Never</th>
</tr>
</thead>
<tbody>
<tr>
<td>Female</td>
<td>11.6%</td>
<td>6.8%</td>
<td>9.8%</td>
<td>71.8%</td>
</tr>
<tr>
<td>Male</td>
<td>16.9%</td>
<td>9.6%</td>
<td>11.8%</td>
<td>61.7%</td>
</tr>
</tbody>
</table>

3.4.7. Newsroom types variable (H7)

H7 expects that types of journalists’ newsrooms influence the digital protection training they receive from their newsrooms. In general, only 7.6% of newsrooms provided digital protection training. Among each category of newsroom types, 10.8% of online-only or digital-only news outlets provided digital protection training, nearly 4 times more compared to 2.4% of journalists in legacy news outlets. Moreover, 7.8% hybrid news outlets that combine legacy and digital news outlets provided digital protection training. The relationship between technical skills and digital protection is statistically significant at p≤.04.

<table>
<thead>
<tr>
<th>% within newsroom type</th>
<th>No</th>
<th>Yes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Legacy news outlet</td>
<td>97.6%</td>
<td>2.4%</td>
</tr>
<tr>
<td>Online-only or digital-only news outlet</td>
<td>89.2%</td>
<td>10.8%</td>
</tr>
<tr>
<td>A hybrid of legacy and digital news outlet</td>
<td>92.2%</td>
<td>7.8%</td>
</tr>
</tbody>
</table>

3.5. Chapter Summary

The above analyses prove the relationship between the following variables and journalists’ use of digital protection: the news content they covered, the media formats they used, their positions in their newsrooms, their technical skills before they got hired by the current
newsrooms, the region in which journalists work, and their gender. I will summarize them in turn.

The analyses reveal that a majority of journalists of each beat rarely or never used digital protection (over 60% of political reporters and economy reporters, over 50% of investigative reporters, and nearly 60% of crime reporters). In general, journalists who covered sensitive and conspicuous topics are more aware of the importance of securing their data, and they do use digital protection more frequently compared to their peers. By contrast, very few local news reporters, including community news and town or city news, regarded digital protection as helpful for them (less than 30% of hyper local and local news reporters respectively).

The analyses also discover that online media journalists tend to use digital protection daily more than their counterparts in legacy news outlets, including printed newspaper, printed magazine, television and radio. Amongst journalists in legacy news outlets, journalists in printed newspapers and television secure their data daily at a higher rate. However, either online media journalists, or newspaper and television journalists, had low percentages of using digital protection daily (around 15% of journalists in online media, printed newspaper and television each). Moreover, full-time journalists in different news outlets are more likely to use digital protection frequently compared to their editorial or freelance peers. In fact, full-time investigative reporters are most likely to secure their data frequently (23.4% used digital protection daily).

The analyses also demonstrate that journalists with technical skills, especially cybersecurity skills, were more likely to secure their data or digital devices. More of the journalists with
cybersecurity skills used digital protection daily, whereas a high proportion of journalists without technical skills rarely or never used digital protection daily.

In addition, the use of digital protection varied across regions and genders. First, very few journalists in western democracies in North America and Europe used digital protection daily. However, their counterparts in Asia had a high percentage of using digital protection. Journalists in other developing regions such as Subsaharan Africa also had a higher percentage than their North American and European counterparts. Second, female journalists used digital protection are less likely than their male counterparts. Given the fact that female journalists were confronted with severe digital surveillance, which result in patricentric insulting and sexualized attacks (Henrichsen, Betz, and Lisosky 2015; Digital Rights Foundation 2017), their less use of digital protection may exacerbate their vulnerability further.

The analyses also provided evidence to support the relationship between newsroom types and journalists’ access to cybersecurity training. Only 7.6% of newsrooms provided cybersecurity training. Moreover, online-only or digital-only newsrooms offered cybersecurity most (10.8% of the online-only or digital-only newsrooms). Still the percentage of newsrooms that offered cybersecurity training overall was rather low.

In the next chapter, I am going to discuss my findings from both the data analyses and literature review further. I will also analyze the possible reasons behind these finding, present opportunity for future studies to explore, and offer recommendations for journalists, newsroom and journalist communities, and policy makers.
Chapter 4. Discussion

In the previous chapter, I presented my finding from the data analyses on the 2019 State of Technology in Global Newsrooms survey. In this chapter, I am going to discuss how my analyses answer three of my research questions in regard to journalists’ use of digital protective measures and the challenges they are confronted with in regard to securing their data. Following the discussion section, a conclusion section will be provided to present the key takeaways from this study, recommendations for various actors to consider, and direction for further studies. These various actors include journalists, newsrooms, the international journalism community, and policy makers.

4.1. How Do Journalists Protect Their Digital Safety?

To answer my first research question, I examined the percentage of journalists using digital protective measures. The analysis shows that a majority (37.2%) of journalists prefer encrypted secure communication over any other measures. Meanwhile, few journalists engaged any of the other protection methods. For instance, less than 15% of journalists used secure email. Still, 22.1% of journalists did not use any digital protective measures. This finding implies that a significant number of journalists did not take any of the possible measures to secure their data or digital devices (Table 9).

<table>
<thead>
<tr>
<th>Digital protective measures</th>
<th>Count</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secure email</td>
<td>399</td>
<td>13%</td>
</tr>
<tr>
<td>Secure phone calls</td>
<td>118</td>
<td>10.4%</td>
</tr>
<tr>
<td>Secure video calls</td>
<td>2146</td>
<td>3.9%</td>
</tr>
<tr>
<td>Secure messaging</td>
<td>2146</td>
<td>37.2%</td>
</tr>
<tr>
<td>VPN</td>
<td>2146</td>
<td>12.8%</td>
</tr>
<tr>
<td>Not secure</td>
<td>2146</td>
<td>22.1%</td>
</tr>
<tr>
<td>Total</td>
<td>3060</td>
<td>100.0%</td>
</tr>
</tbody>
</table>

This finding is slightly different from the 2015 United Nations report I discussed in my literature review (Henrichsen, Betz, and Lisosky 2015). Henrichsen, Betz, and Lisosky discovered that journalists were actively using encrypted emails and messaging, document
encryption, VPN and encrypted cloud storage. However, very few respondents of the 2019 State of Technology in Global Newsrooms survey, which I used for my secondary data analyses, reported that they used document encryption and encrypted cloud storage as their form of protection. This may indicate a change in journalists’ use of digital protective measures from 2015 to 2019. It may also be a result of differences in the samples employed by the two studies, as the 2019 State of Technology survey had broader representation of the journalism field.

Despite the fact that some journalists have taken some measures to secure their data, a majority of journalists rarely or never took measures to protect their digital safety, accounting for 60% of the respondents (Table 10). This finding is worrisome, since the lack of digital protective measures may compound their vulnerability. Journalists are exposed to the highest risks of being surveilled compared to their editorial peers. For example, female journalists in Pakistan reported that they have more exposure to social surveillance because they have to go to the spot for investigation, present on the TV, or appear on the newspaper where they have their name. This makes them easier to be targeted by the state and malicious actors. By contrast, their editors work behind the scenes and stay low key, which exposes them to less risks of being surveilled (Digital Rights Foundation 2017).

Table 11. Journalists’ Frequency of Using Digital Protective Measures

<table>
<thead>
<tr>
<th>Frequency</th>
<th>Valid Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Daily</td>
<td>320</td>
</tr>
<tr>
<td>Weekly</td>
<td>182</td>
</tr>
<tr>
<td>Monthly</td>
<td>246</td>
</tr>
<tr>
<td>Rarely/Never</td>
<td>1398</td>
</tr>
<tr>
<td>Total</td>
<td>2146</td>
</tr>
</tbody>
</table>

In addition, journalists’ use of digital protective measures decreased by 20 percentage points from 2017 to 2019 (ICFJ 2019; ICFJ 2017). There may be three possible reasons. First, journalists are becoming more complacent about their digital safety, and they find it unnecessary to take protective measures for their data and digital devices. Second, there has been a lack of
widely known cases such as the Snowden files that involve digital surveillance in recent years, which reduces journalists’ attention to their digital safety. Third, with the surging number of digital surveillance and malware attacks, journalists feel like they are always being watched even if they try to secure their data (Waters 2018), and therefore some of them decide not to use protective measures.

4.2. What Influences Journalists’ Use of Digital Protective Measures?

My second research question is answered by the analyses for H1 through H5. The analyses indicate that journalists’ use of digital protective measures is related to the news content they covered most often, the media formats they used, their positions in their newsrooms, their technical skills before they were hired by the current newsrooms, the regions in which journalists work, and their gender. Some of my findings show some discrepancies with existing literature. For instance, Waters (2018) and Tsui and Lee (2019) found that journalists who covered sensitive topics, including investigative reports, politics, and crime, are more aware of the importance of digital safety, but my analyses show that these same journalists do not necessarily secure their data. The percentages of political and crime reporters using digital protective measures daily are similar to the percentage of journalists covering the economy, which is not considered to be sensitive. Meanwhile, journalists who never protected their digital safety are nearly 60% of investigative, political, and crime reporters.

In addition, most of my data analyses for my second research question are parallel to some findings in the literature. For example, Mills (2019) believed that journalists in relatively democratic countries have less concern about surveillance. This comports with some of my analyses that western democracies have the lowest percentage of journalists who took measures to protect their digital safety among different regions. Over 70% of the journalists in Europe and North America never or rarely used digital protective measures. In contrast, journalists in South
Asia, East and Southeast Asia, and Subsaharan Africa regions used digital safety in a higher rate (30%, 18.5%, and 17.1% respectively). The reason for this finding may be explained by Mills (2019) that journalists located in these three regions were confronted with more digital surveillance and interrogation resulting from the surveillance conducted by repressive regimes, compared with their peers in democratic countries, such as western Europe and the United States of America. Still, the lack of digital protective measures among journalists in western democracies may result in further erosion of freedom of speech and democracy, as Mills has warned in her study. As digital surveillance has expanded the power of government and restricted journalists’ activities, traditional “watchdog” journalism can no longer keep government power in check.

In general, the situation of vulnerable groups among journalists is alarming. Female journalists, as well as investigative, crime or political reporters, used digital protection at very low rates. (1) Female journalists were less likely to secure their data by a difference of 5 percentage points (11.6%). There was a 10-percentage point difference between female and male journalists who never secure their data. The percentage of women who never used digital protective measures was higher than for men (71.8%). (2) 20.7% of investigative reporters, 16.3% of political journalists, and 18.4% of crime reporters used digital protection daily. This indicate a very small number among them to secure their data with protective measures. That is to say, their vulnerabilities to digital surveillance and malware attacks could be compound by their lack of protective measures.

4.3. What Challenges Do Journalists Face in Their Efforts to Protect Their Digital Safety?

To answer my third research question, I conducted a crosstab analysis and examined cybersecurity training offered by newsrooms. The analyses indicate that journalists’ efforts to secure their data may be challenged by their low awareness of cybersecurity, their lack of technical skills, and their limited access to organizational training. Furthermore,
newsrooms’ offerings in cybersecurity training also have a discrepancy with journalists’ preference for the training formats. However, this research question is not completely answered by the analyses, as it requires further studies to cover a broader picture of various challenges journalists are confronted with in efforts to secure their data.

4.3.1. Cybersecurity awareness
My analyses disclosed that only 27.1% of journalists believed cybersecurity is the most helpful type of training for them among various skills (Table 11). This may explain why nearly 70% of journalists in the survey claimed that they rarely or never used digital safety (Table 10), as both Waters (2018) and Tsui and Lee (2019) suggested that journalists with higher awareness of digital safety are more likely to secure their data compared to their peers. Based on this, we may need more educational intervention for journalists to take actions and secure their data. In other words, increasing journalists’ awareness of cybersecurity may be an important step in protecting them from digital surveillance and attacks.

<table>
<thead>
<tr>
<th>Table 12. Journalists’ Use of Digital Protective Measures</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
<tr>
<td>No</td>
</tr>
<tr>
<td>Yes</td>
</tr>
</tbody>
</table>

4.3.2. Technical skills
The analysis for H4 shows that the lack of technical skills poses challenges for journalists using digital protective measures (Table 5). In general, the majority of journalists without technical skills rarely or never used digital protective measures, and most of the newsrooms did not provide cybersecurity training for journalists. Journalists’ lack of proficiency in technical skills, particularly cybersecurity skills, may result from their low awareness of available technology for them to secure their data and the lack of organization support.

4.3.3. Organizational support
Some of the findings from the literature demonstrate that organizational support offered by newsrooms for their journalists to secure their data include cybersecurity training, provision of
digital safety tools and workflows of securing digital communication, and technical consulting (Waters 2018; Digital Rights Foundation 2017). However, my analyses discovered that a majority of newsrooms took no responsibility for journalists protecting their digital safety. As Table 12 shows, only 7.6% of newsrooms managers reported that their newsrooms provide cybersecurity training. In particular, online-only or digital-only newsrooms are more likely to provide cybersecurity training than their hybrid or legacy news counterparts (Table 13). Based on this finding, it may be possible that the lack of organization training is one challenge for journalists to protect their digital safety. This may be because legacy news outlets do not have a culture of securing their data and digital devices, because they were established way ahead of the digital era. This may also be the case for hybrid newsrooms that combine traditional and digital news outlets. For instance, some hybrid newsrooms are transformed from legacy news outlets, and they use digital media as well as other legacy news outlets to distribute their news stories. Still, they focus on legacy media outlets, which take away their own attention to protect their digital information. By contrast, it is easier for digital-only or online-only newsrooms to attract the attention of governments and malicious actors to conduct digital surveillance or malware attacks.

| Table 13. Whether Journalists’ Newsrooms Provide Cybersecurity Training |
|---------------------------------|----------------------|-------------------------|
| Frequency | Valid Percent |
| No         | 971            | 92.4%                  |
| Yes        | 80             | 7.6%                   |

| Table 14. Whether Journalists’ Newsrooms Provide Cybersecurity Training |
|---------------------------------|----------------------|-------------------------|
| Online-only or digital-only news organization | Frequency | Valid Percent |
| 4                                      |           | 5.1%             |
| A hybrid of traditional and digital news organization | 42       | 53.8%             |
| Total                                 | 885       | 100%              |
To understand the effectiveness of particular types of cybersecurity training, two analyses of the frequency of journalists’ preferred formats of cybersecurity training and formats of existing cybersecurity training provided by newsrooms were conducted on my dataset. My analyses illustrate that 43.6% of journalists think a hands-on format including intensive workshops and lab sessions is effective. However, few journalists prefer online (17.2%) or peer-to-peer sessions (3.8%). Therefore, the format of hands-on, intensive workshops and lab sessions is the most preferable among journalists. In addition, a small percentage of journalists prefer multi-day and online training (17.9%; 17.2%). However, the preferences of journalists differ from the existing format of cybersecurity training provided by newsrooms. In particular, my analyses show that hands-on sessions and short classes are the most commonly used formats of cybersecurity training that are provided by newsrooms (Table 15). This may suggest a gap between journalists’ expectations and newsrooms’ offering in cybersecurity training.

<table>
<thead>
<tr>
<th>Training format</th>
<th>Count</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Short classes (half day or less in duration)</td>
<td>62</td>
<td>7.7%</td>
</tr>
<tr>
<td>Single-day classes</td>
<td>55</td>
<td>3.6%</td>
</tr>
<tr>
<td>Hands-on, intensive workshops and lab sessions</td>
<td>353</td>
<td>43.6%</td>
</tr>
<tr>
<td>Multi-day training institutes</td>
<td>145</td>
<td>17.9%</td>
</tr>
<tr>
<td>Peer-to-peer meeting</td>
<td>31</td>
<td>3.8%</td>
</tr>
<tr>
<td>Online training</td>
<td>139</td>
<td>17.2%</td>
</tr>
<tr>
<td>Total</td>
<td>1192</td>
<td>100.0%</td>
</tr>
</tbody>
</table>

Table 16. Formats of Cybersecurity Training Offered by Newsrooms

<table>
<thead>
<tr>
<th>Training format</th>
<th>Count</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Single-day classes</td>
<td>31</td>
<td>38.8%</td>
</tr>
<tr>
<td>Hands-on, intensive workshops and lab sessions</td>
<td>46</td>
<td>57.5%</td>
</tr>
<tr>
<td>Short classes (half day or less in duration)</td>
<td>44</td>
<td>55.0%</td>
</tr>
<tr>
<td>Multiple-day classes</td>
<td>30</td>
<td>37.5%</td>
</tr>
<tr>
<td>Online training</td>
<td>32</td>
<td>40.0%</td>
</tr>
<tr>
<td>Peer-to-peer meeting</td>
<td>32</td>
<td>40.0%</td>
</tr>
</tbody>
</table>

However, the above analyses only explore part of the challenges that journalists face in their endeavors to protect their digital safety. Henrichsen, Betz, and Lisosky (2015) believed that
journalists were confronted with various challenges, such as the decline of newsroom profits, the evolving nature of surveillance technologies, and an increasing ease of conducting malware attacks. That is to say, more studies need to be conducted to fully answer my third research question. The following section will provide some directions for future studies.
Chapter 5. Conclusion

This section will present the key takeaways of this study. These takeaways include my findings via existing literature and data analyses. Based on the key findings, I will provide my recommendations for journalists, their newsrooms, global journalist communities and policy makers to address the digital safety issues of journalists. Some directions for future studies will also be provided in this section.

5.1. Key Takeaways of This Study

The key takeaways of this study are as follows:

- **Consequences:** Digital surveillance have posed threats to journalists’ personal safety, and resulted in self-censorship of journalists and newsrooms. It has generated far-reaching consequences, including breaches of civil rights, erosion of freedom, and challenge to political democracy.

- **Digital surveillance and malware attacks are intersected at times.** Malware attacks create access for digital surveillance of journalists and vice versa. This can be demonstrated by the example of the Saudi Arabic journalist Jamal Khashoggi (Sant 2018; Kenyon 2018) as well as Henrichsen, Betz, and Lisosky’s (2015) study.

- **A majority of journalists have a very low awareness of digital safety and a lower frequency of using digital protective measures.** Nearly 70% of journalists rarely or never used digital safety. Only 27.1% of journalists regarded cybersecurity training is the most helpful type of training. Given the consequences of digital surveillance and malware attacks on journalists, which have been referenced in my literature review, their lack of digital protective measures has become a vital issue.
• Journalists’ use of digital protective measures is closely related to (1) the news content they covered most often, (2) the media formats they used, (3) their positions in their newsrooms, (4) their technical skills before they were hired by the current newsrooms, (5) the region in which journalists work, and (6) their gender.

(1) The news content: journalists who covered sensitive and conspicuous topics are more aware of the importance of securing their data, and they do use digital protection more frequently compared to their peers. In contrast, very few local news reporters, including community news and town or city news, regarded digital protection as helpful for them.

(2) The media formats they used: online media journalists tend to use digital protection daily more than their counterparts in legacy news outlets, including printed newspaper, printed magazine, television and radio. Amongst journalists in legacy news outlets, journalists in printed newspapers and television secure their data daily at a higher rate. However, either online media journalists, or newspaper and television journalists, had low percentages of using digital protection daily.

(3) Their newsroom positions: 70.4% of freelance journalists rarely or never used digital protective measures. This indicates that the vulnerable groups among journalists did not secure their data, and this will exacerbate their vulnerability to digital surveillance and malware attacks.

(4) Their technical skills before they were hired by the current newsrooms: 80% of journalists who have no technical skills never or rarely used digital protective measures, 4 times more than the 17.8% of journalists having digital protective
measures skills. Journalists with cybersecurity skills are most likely to secure their data. 38.7% of journalists with cybersecurity skills used digital protective measures daily, more than twice as many as journalists with other skills, such as skills in digital video, audio or photo tools and skills in researching or distributing stories via social media.

(5) The region in which journalists work: Over 70% of the journalists in Europe and North America never or rarely used digital protective measures. As Mills (2019) claimed in his study, the capability of digital surveillance in western democracies has been expanded both legally and technically, resulting in a severe digital surveillance of journalists. Given this situation, the digital safety of journalists in western democracies will be further compromised due to their lack of digital protective measures.

- Nearly 95% of the newsrooms did not offer cybersecurity training for their journalists. In fact, legacy newsrooms or hybrid newsrooms are less likely to offer the training compared with online-only or digital-only newsrooms. This situation also is alarming. Newsrooms should establish a support system for their journalistic staff, including cybersecurity training.

5.2. Recommendations
In this section, I will provide my recommendations in light of the findings from extant literature and data analyses. As their digital safety has become a vital issue, journalists should take protective measures to secure their data and devices. Various stakeholders, particularly newsrooms, global journalist communities, and policy makers, also need to raise their awareness (awareness is not for themselves) and contribute more efforts in the protection of journalists’ digital safety. They may consider the following recommendations.
5.2.1. Journalists

Journalists need to be aware of their vulnerability to digital surveillance and malware attacks, and take effective actions to address the issue:

- Journalists should continually attend cybersecurity training, so they can stay informed of the latest types of digital surveillance and malware attacks as well as the possible strategies to secure their data.
- Journalists need to use various protective measures simultaneously to secure their data. For instance, journalists may connect with VPN when using encrypted emails or messaging.
- Journalists may request more access to supportive resources from their newsrooms, including cybersecurity training, digital safety toolkits and technical advice. They could consider organizing their own unions to request these resources.
- Journalists should build up strong communities to share their experiences with each other. These communities could also share protective resources, such as the shared use of digital safety tools and technical consulting.

5.2.2. Newsroom

Protecting the digital safety of journalists is also a worthwhile investment for newsrooms. A support system for journalism staff benefits newsrooms’ reputation of professionalism in two ways: (1) It shapes their image of caring about their employees and protecting their sources; (2) It creates more opportunities for newsrooms to cover those sensitive, controversial and conspicuous topics with fewer risks of giant malware attacks and shutting down their investigative reports (Tsui and Lee 2019). Based on these reasons, newsrooms need to play an active role in creating a secure professional environment for their journalists. To achieve these goals, journalists need to:
• Create a support system for journalists to ensure their digital safety. The support system should provide sufficient access to (1) digital safety training, (2) protection tools, or (3) technical guidelines. (1) Digital training may be normalized in the formats of hands-on, intensive workshops and lab sessions, which journalists suggested as the most effective training formats in this study. (2) Protection tools should help journalists to secure their digital communication and devices, documents and internet connections. These tools include encrypted messaging and emails, secure audio or video calls, company VPN and encrypted document storages. This recommendation is based on the findings of this study and the reports by Waters (2018) and Henrichsen, Betz, and Lisosky (2015). (3) Technical guidelines may be implemented via regular workflows that require the use of digital protective measures (Waters 2018). They can also be offered as technical advice by cybersecurity professionals.

• The support system should establish a mechanism, such as a hotline, survey forms or websites, for journalists to report digital surveillance or malware attacks (Article 19; Henrichsen, Betz, and Lisosky 2015; Digital Rights Foundation 2017). The mechanism should facilitate newsrooms’ communication and collaboration with policy makers and journalist communities.

• The support system should also create a secure and friendly environment for journalists to seek comfort by self-disclosing trauma caused by digital surveillance and attacks, as well as gain professional assistance (Digital Rights Foundations 2017). This requires newsrooms to work with journalist communities and policy makers.

5.2.3. Journalist communities and policy makers
Shielding journalists from digital threats is vital to protect civil rights and freedom as well as ensure the sustainability of democracy (Mills and Sarikakis 2016). This requires efforts from
various stakeholders, particularly journalist communities and policy makers. These two stakeholders share some similarities in their roles. For instance, both of them have established normative frameworks to protect journalists’ digital safety. They also carry the potential to offer inter-organizational support for journalists and their newsrooms. My recommendations for them are listed as follows:

- Journalist communities and policy makers should work with ISPs to ensure the protection of users’ privacy, which is closely related to journalists’ digital safety. Particularly, policy makers may consider: (1) Requiring ISPs to increase protection for sensitive personal data stored in their servers. (2) Monitoring the violation of privacy across internet platforms. (3) Providing legal remedies for journalists whose privacy rights are infringed by internet service providers.

- Journalist communities and policy makers should provide support for newsrooms with limited access to resources. The support may include funding, training resources and technical consulting for newsrooms to build up their support systems for the digital safety of their journalistic staff.

- Journalist communities and policy makers should tackle mass surveillance and malware attacks targeting journalists. The report of Digital Rights Foundation (2017) shows that journalists were confronted with mental traumas resulting from digital surveillance and malware attacks. To help journalists tackle their mental issues, (1) journalist communities need to cooperate with their newsrooms to create a friendly culture that encourages sharing and discussing, and (2) Policy makers should abolish legal frameworks that “arbitrarily arrest or detain journalists, and release those in detention” (Article 19 2017: 15), remove state surveillance of journalists for national security purposes, and ensure an environment for journalists to fulfill their jobs independently.
• Given the evolving nature of digital surveillance or malware attacks (Henrichsen, Betz, and Lisosky 2015), journalist communities and policy makers should collaborate with technology developers to develop advanced technology for journalists to secure their data.

• Journalist communities and policy makers need to understand the evolving nature of journalism. This would help to provide digital safety protection for non-traditional journalists (Digital Rights Foundation 2017). As I discovered in this study, as part-time and freelance journalists working for online or digital media, as well as citizen journalists are more vulnerable than their peers working in legacy news outlets or on a full-time basis. Most of them rarely or never receive organizational support from newsrooms to protect their digital safety.

• Journalist communities and policy makers should enhance protective measures for vulnerable groups amongst journalists. This also requires them to consider social and legislative contexts that increase the vulnerability of certain groups, such as female or investigative reporters and journalists coming from minority religious and ethnic groups. Journalist communities should also pay attention to journalists located in areas where certain protective measures, such as VPN, are outlawed – prohibited by the local laws.

• Journalist communities and policy makers should enforce the requirements of normative or legal frameworks in newsrooms.

  (1) Newsrooms should be held accountable for compliance with requirements, guidelines, and instructions that ensure journalists’ digital safety. Newsrooms that do not follow these requirements should be fined.

  (2) Policy makers and journalist communities should ensure that frameworks ensuring journalists’ digital safety are legally binding. These frameworks should make sure that digital attackers are punished, and victims receive legal remedies.
5.3. Limitations

This study has four distinct limitations. First, the data does not show how journalists address different digital threats. As the literature shows, journalists are confronted with breaches of their privacy (Mills and Sarikakis 2016), online abuse or harassment, and digital surveillance (Henrichsen, Betz, and Lisosky 2015). These are separate forms of the digital threats posed to journalists. There is also no differentiation between the threats based on journalists’ professional or personal identities on the dataset.

Second, it is beyond the scope of this study to examine contexts within different countries that can account for journalists’ vulnerabilities. Mills (2019) believed that journalists’ vulnerabilities to digital surveillance vary across democracies, limited democracies, repressive societies, and authoritarian regimes. My data analyses of this study, however, do not provide records of this possible division. For example, the data analyses do not explain how the legislative context affects journalists’ frequency of using certain digital protective measures, as is referenced in the literature review. My analyses also do not illustrate whether legacy news or hybrid outlets offer more cyber training in democratic societies than their counterparts in repressive regimes.

Meanwhile, my data analysis only focuses on regional differences of journalists’ vulnerabilities to digital attacks and does not allow for precise conclusions for perceived threats of journalists across countries, including investigative reporters and female journalists. For instance, there may be a much higher likelihood for investigative reporters in democratic societies to receive more cybersecurity training than their peers in repressive regimes. Another example is female journalists’ use of digital safety by countries. My data analyses support the finding from the extant literature that in general female journalists used digital protection daily at a lower rate compared to their male counterparts. But the current data analyses do not provide a clear explanation about whether female journalists in certain regions are particularly vulnerable
due to social-cultural factors compared to female journalists in other countries. For example, the report from Digital Rights Foundation (2017) shows that female journalists in Pakistan were subject to gender-based surveillance on social media, particularly those with a background of minority ethnic or marginalized religious and political groups.

Third, my data analyses do not provide a comprehensive analysis exploring the challenges journalists are confronted with in efforts to ensure their digital safety. My data analyses show that only 7.6% of newsrooms offered cybersecurity training, which may be one challenge journalists face. Yet the analyses do not investigate other challenges, such as the reduced costs of conducting malware attacks, the evolving nature of surveillance technologies (Henrichsen, Betz, and Lisosky 2015), and the learning curve of installing digital protection equipment (Waters 2018).

Fourth, my data analyses do not present how ISPs have caused actual or possible threats to journalists’ digital safety. This specific issue should be a subject to future research.

5.4. Directions for Future Studies

In the next step for research, more studies need to be conducted to understand the various challenges with which journalists are confronted in their efforts to protect their digital safety. For example, a survey may be conducted to inquire about journalists’ feelings about the challenges they face. Moreover, some qualitative interviews may be carried out to understand the context of journalists’ challenges to protect their digital safety. Meanwhile, further studies may investigate whether newsrooms provide various types of organizational support for journalists to secure their data, such as technical guidelines, company security tools and security workflows. Future studies also may examine how the lack of organizational support challenges journalists’ efforts to protect their digital safety.

Future study may also explore in what ways internet service providers could pose threats
to journalists’ digital safety. As is referenced in the literature review, ISPs may either provide easy access for third-party actors to detain and manipulate user data or violate user privacy themselves (Mills and Sarikakis 2016; Gellman and Poitras 2013; Venkatadri et al. 2019).

Future studies may also provide a comprehensive view of how journalists may defend their digital safety in various political and social-cultural contexts. These contexts may include: (1) social-cultural contexts that are related to journalists’ social identities, such as their gender or religious, ethnic, class or political identities, and (2) legislative contexts that directly determine journalists’ vulnerability to digital surveillance and malware attacks, such as the enforcement of state surveillance, censorship or internet control. Researchers may study journalists whose vulnerability has been exacerbated in these contexts and develop feasible strategies for them and their newsroom to enhance their digital safety.
Appendix I. Glossary

- Digital surveillance: To have forced access or keep watching people’s digital devices to collect and store their information or monitor their activities (Henrichsen, Betz, and Lisosky 2015; Waters 2018; Digital Rights Foundations).

- Software-as-a-service (SaaS): A service that allows “data to be accessed from any device with an internet connection and a web browser. In this web-based model, software vendors host and maintain the servers, databases, and the code that makes up an application” (Softwareadvice.com 2020).

- Infrastructure-as-a-service (IaaS): A service that “manages the infrastructure, while you purchase, install, configure, and manage your own software—operating systems, middleware, and applications” (Microsoft Azure n.d.).

- Legacy news outlets: news outlets that include printed media, film studios, music studios, advertising agencies, radio broadcasting, and television (Henrichsen, Betz, and Lisosky 2015).

- Watchdog journalism: It aims to “inform the public about goings-on in governmental institutions and society, especially in circumstances where a significant portion of the public would demand changes in response” (Wikipedia 2019).

- Non-traditional journalism: a type of journalism that uses digital or online news outlets or employs non-traditional journalists, such as part-time or freelance reporters, bloggers, new media content creators and citizen journalists (Digital Rights Foundation 2017; Mills and Sarikakis 2016; Henrichsen, Betz, and Lisosky 2015).

- ISP: internet service providers (Mills and Sarikakis 2016).
Appendix II. Survey Questionnaire

The following survey is from the cybersecurity section of the 2019 State of Technology in Global Newsrooms (ICFJ 2019).

1. The International Center for Journalists (ICFJ) invites you to participate in our survey on the State of Technology in Global Newsrooms. You are being asked to take part in this survey because you are a journalist. The survey is being conducted worldwide and is available in 14 languages.

The study will update and expand ICFJ's 2017 State of Technology in Global Newsrooms report—the first of its kind to shed light on how news outlets and journalists are evolving to meet the demands of the digital era. ICFJ will produce a new report based on the findings of the current survey. We greatly appreciate your participation in this important study that will benefit journalists worldwide. This survey will take 15-20 minutes to complete.

Respondents can enter a drawing and win one of 30 $100 Amazon gift cards. If you are interested in additional data analysis beyond the published report, we invite you to contact the principal researcher, Dr. Diana Owen, Professor, Georgetown University at owend@georgetown.edu.

Google News Initiative and Fusion are providing generous support for this survey.

2. Is your role primarily as a news manager/executive or a journalist?
   o Manager/Executive
   o Journalist

3. Which of the following best describes your newsroom?
   o Traditional news organization (relies primarily on print or broadcast to distribute content)
   o Online-only or digital-only news organization
   o A hybrid of traditional and digital news organization
   o Other (please specify)

4. In what format does your organization PRIMARILY disseminate news?
   o Print newspaper
   o Television
   o Print magazine
   o Radio
   o Website
   o News App
   o Podcast
   o Email newsletter
   o Other (please specify)

5. Which of the following best describes your position in the newsroom?
   o Investigative Reporter
   o Beat Reporter
   o News Reporter
   o Feature Writer
   o Editorial Writer
   o Top Editorial Leadership or Executive Fact-Checker
   o Photojournalist
   o Video Producer/Editor
   o Audio Producer/Editor
   o Digital Content Producer/Editor
   o Design or Multimedia Professional
   o Social Media Editor
   o Technology Professional (Software and tool development) Analytics Editor/Professional
o Cartoonist (such as a political cartoonist)
o I do not work in a newsroom
o Other (please specify)

6. What type of news do you cover most often?
o Hyper local (e.g. community news)
o Local (e.g. town or city news)
o National news Regional news
o Other (please specify)
o International news
o Some combination of local, regional, national, and international news

7. Which of the following beats or content areas do you cover most often? Please check all that apply.
o Agriculture
o Business and Commerce
o Crime and Courts
o The Economy
o Education
o Energy
o Entertainment
o Government and Politics
o Health
o Other (please specify)
o Investigative Reports Labor
o Lifestyle
o Opinion
o Poverty and Development
o Religion and Faith
o Sports
o Technology
o Weather
o I do not cover news

8. How often do you use the following technical skills in your position in the newsroom? (Daily, Weekly, Monthly, Rarely/Never)
o Cybersecurity

9. What type of TECHNICAL SKILLS TRAINING would be most helpful for you? Please check all that apply.
o Audio production and editing
o Video production and editing
o Website and page layout
o Website development
o Working with live video
o Working with VR/360
o Podcast production
o Creating visuals (animations, gifs)
o Building or adapting digital tools/apps for newsroom use
o Other (please specify)
o Using artificial intelligence (AI) and robo-journalism
o Mobile and backpack reporting
o Using a content management system for newsrooms
Using tools to verify and fact-check information
Understanding and using data analytics
CMS management and coding
Search engine optimization (SEO)
Cybersecurity
I do not need technical skills training

10. What training format is the most effective?
- Short classes (half day or less in duration)
- Single day classes
- Hands-on, intensive workshops and lab sessions
- Multi-day training institutes
- Other (please specify)
- Peer-to-peer training
- Online training
- No preference

11. Do you use any of the following to secure your communication? Please check all that apply.
- Email encryption (like Hushmail, Mailvelope)
- Chat encryption (like Chat Secure, Cryptocat)
- Phone call encryption (like Signal)
- Video conference encryption (like Jitsi)
- Other (please specify)
- Secure messaging services (WhatsApp, Telegram, Signal)
- Personal/Company VPN
- I do not secure my communication

12. What is your gender?
- Female
- Male
- Non-binary

13. In which regions are you located?
- Latin America/Caribbean
- Middle East/North
- Africa
- SubSaharan Africa
- East and Southeast Asia
- South Asia
- Europe
- North America
Works Cited


