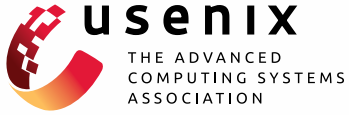

Investigating the Computer Security Practices and Needs of Journalists

Susan E. McGregor, ***Columbia Journalism School;*** **Polina Charters, Tobin Holliday, and Franziska Roesner,** ***University of Washington***

https://www.usenix.org/conference/usenixsecurity15/technical-sessions/presentation/mcgregor

This paper is included in the Proceedings of the 24th USENIX Security Symposium

August 12–14, 2015 • Washington, D.C.

ISBN 978-1-939133-11-3

Open access to the Proceedings of the 24th USENIX Security Symposium is sponsored by USENIX

Investigating the Computer Security Practices and Needs of Journalists

Susan E. McGregor
Tow Center for Digital Journalism
Columbia Journalism School

Polina Charters, Tobin Holliday
Master of HCI + Design, DUB Group
University of Washington

Franziska Roesner
Computer Science & Engineering
University of Washington

Abstract

Though journalists are often cited as potential users of computer security technologies, their practices and mental models have not been deeply studied by the academic computer security community. Such an understanding, however, is critical to developing technical solutions that can address the real needs of journalists and integrate into their existing practices. We seek to provide that insight in this paper, by investigating the general and computer security practices of 15 journalists in the U.S. and France via in-depth, semi-structured interviews. Among our findings is evidence that existing security tools fail not only due to usability issues but when they actively interfere with other aspects of the journalistic process; that communication methods are typically driven by sources rather than journalists; and that journalists' organizations play an important role in influencing journalists' behaviors. Based on these and other findings, we make recommendations to the computer security community for improvements to existing tools and future lines of research.

1 Introduction

In recent decades, improved digital communication technologies have reduced barriers to journalism worldwide. Security weaknesses in these same technologies, however, have put journalists and their sources increasingly at risk of identification, prosecution, and persecution by powerful entities, threatening efforts in investigative reporting, transparency, and whistleblowing.

Recent examples of such threats include intensifying U.S. leak prosecutions (e.g. [46, 54]), the secret seizure of journalists' phone records by the U.S. Justice Department [55], the collection of journalists' emails by the British intelligence agency GCHQ [11], politically-motivated malware targeting journalists (among others) [13, 36, 41, 45], and other types of pervasive digital surveillance [34]. In the U.S., these developments have led to a documented "chilling effect", leading sources to reduce communication with journalists even on non-sensitive issues [25, 40]. Elsewhere, risks to journalists and sources cross the line from legal consequences to the potential for physical harm [42, 57, 58].

Responses to these escalating threats have included guides to best computer security practices for journalists (e.g., [17, 43, 47, 62]), which recommend the use of tools like PGP [67], Tor [22], and OTR [14]. More generally, the computer security community has developed many secure or anonymous communication tools (e.g., [4, 10, 14, 21–23, 63, 67]). These tools have seen relatively little adoption within the journalism community, however, even among the investigative journalists that should arguably be their earliest adopters [48].

To design and build tools that will successfully protect journalist-source communications, it is critical that the technical computer security community understand the practices, constraints, and needs of journalists, as well as the successes and failures of existing tools. However, the journalistic process has not been deeply studied by the academic computer security community. We seek to fill that gap in this paper, which is the result of a collaboration between researchers in the journalism and computer security communities, and which is targeted at a technical computer security audience.

To achieve this, we develop a grounded understanding of the journalistic process from a computer security perspective via in-depth, semi-structured interviews. Following accepted frameworks for qualitative research [18, 30, 35], we focus closely on a small number of participants. We interviewed 15 journalists employed in a range of well-respected journalistic institutions in the United States and France, analyzing these interviews using a grounded theory approach [18, 30]. We then synthesize these findings to shed light on the general practices (Section 4.3), security concerns (Section 4.4), defensive strategies (Section 4.5), and needs (Section 4.6) of journalists in their communications with sources.

Our interviews offer a glimpse into journalistic processes that deal with information and sources of a range of sensitivities. Some of our participants report being

the direct targets of threats like eavesdropping and data theft: for example, one participant received threatening letters and had his laptop (and nothing else) stolen from his home while working on sensitive government-related stories. Others discuss their perceived or hypothetical security concerns, which we systematize in Section 4.4 — along with threats that participants tended to overlook, such as the trustworthiness of third-party services.

By cataloguing the computer security tools that our participants do and don't use (Section 4.5), we reveal new reasons for their successes or failures. For example, built-in disk encryption is widely used among our participants because it is both easy-to-use and does not require explicit installation. However, we find that many security tools are not used regularly by our participants. Beyond the expected usability issues, we find that the most critical failures arise when security tools interfere with another part of a journalist's process. For example, anonymous communication tools fail when they compromise a journalist's ability to verify the authenticity of a source or information. As one participant put it: *"If I don't know who they are and can't check their background, I'm not going to use the information they give."* This requirement limits the effectiveness even of tools developed specifically for journalists — such as SecureDrop [26], which supports anonymous document drops — and highlights how crucial it is for computer security experts who design tools for journalists to understand and respect the requirements of the journalistic process.

Based on our findings, we make recommendations for technical computer security researchers focusing on journalist-source communications, including:

- *Focus on sources:* Journalists often choose communication methods based on sources' comfort with and access to technology, rather than the sensitivity of information — particularly when sources are on the other side of a "digital divide" (e.g., low-income populations with limited access to technology).
- *Consider journalistic requirements:* Security tools that impede essential aspects of the journalistic process (e.g., source authentication) will struggle to see widespread adoption. Meanwhile, unfulfilled technical needs (e.g., the absence of a standard knowledge management tool for notes) may cause journalists to introduce vulnerabilities into their process (e.g., reliance on third-party cloud tools not supported by their organization). These unfulfilled needs, however, present opportunities to integrate computer security seamlessly into new tools with broader applicability to the field of journalism.
- *Beyond journalist-source communications:* A journalist's organization and colleagues play an important role in the security of his or her practices; security tools must consider this broader ecosystem.

We consider these and other lessons and recommendations in more detail below. Taken together, our findings suggest that further collaboration between the computer security and journalism communities is critical, with our work as an important first step in informing and grounding future research in computer security around journalist-source communications.

2 Related Work

We provide context for our study through a survey of three types of related works: studies of journalists and computer security, computer security guidelines developed specifically for journalists, and secure communication tools.

Studies of journalists and computer security. Several recent studies interviewed or surveyed journalists (among others) in Mexico [58], Pakistan [42], Tibet [15] and Vietnam [57] to shed light on the risks associated with their work, as well as their use and understanding of computer security technologies (such as encryption). Despite the different context, our findings echo some of the findings in these studies: for example, that maintaining communication with sources may take precedence over security [57], that meeting in person may be preferable to digital communication [15], and that the use of more sophisticated computer security tools is typically limited even in the face of real threats, including risk of physical harm [42, 57, 58]. These prior studies primarily recommended increased computer security education and training for journalists; though we concur, our work focuses more on technical recommendations.

Though most journalists in countries like the United States do not face physical harm, recent interviews of U.S. journalists and lawyers [40] revealed a distinct chilling effect in these fields resulting from revelations about widespread government surveillance. For example, journalists reported increased reluctance by sources to discuss even non-sensitive topics. Another recent report [48] provides quantitative survey data about the use of computer security tools by investigative journalists, suggesting (as we also find) that sophisticated computer security tools have seen limited adoption. These studies begin to paint a picture of the computer security mental models and needs of journalists; we expand on that understanding in this work and distill from it concrete technical and research recommendations.

The computer security community has previously studied the usability and social challenges with encryption among other populations (e.g., [27, 65]). Where applicable, we draw comparisons or highlight differences to the findings of these works.

Computer security guidelines for journalists. Recent concerns about government surveillance have prompted

journalists in the U.S. and elsewhere to weigh computer security more seriously. For example, several groups have developed computer security guidelines and best practices for journalists [17, 43, 47, 62]. Online guides for journalists and other technology users (e.g., [16]) also abound. These efforts highlight the need for engagement between the journalism and computer security communities, but generally take the approach of educating journalists to use existing available tools, such as GPG and Tor. The goal of our work is to provide the developers of new technologies with a deep, grounded understanding of the needs and security concerns of journalists.

Secure communication. A large body of work exists on secure communication and data storage, both commercially and in the computer security research literature. For example, various smartphone applications aim to provide secure text messaging or calling [6, 60, 64]; a range of desktop applications provide disk encryption and cleaning [1, 5, 8]; Tor [22, 61] aims to provide anonymous web surfing; Tails [4] aims to provide a private and anonymous operating system; and tools like GPG and CryptoCat provide encryption for email and chat messages respectively [2, 31]. Several email providers have also attempted to provide secure and anonymous email [3, 44]. Though valuable, most of these tools and techniques have known weaknesses: anonymous email, for example, lacks essential legal protections [38, 51]. Tor and Tails do not protect against all threats and present usability challenges (e.g., [49]). Finally, many applications that appear to provide certain security properties fail to provide those guarantees in the face of government requests [33, 56].

While the above-mentioned commercial tools are among those frequently recommended to journalists, the computer security research community has also considered anonymous communications in depth. These efforts include developing, analyzing, and attacking systems like trusted relays, mix systems, and onion routing such as that used in Tor. Good summaries of these bodies of work can be found in [21] and [23]. Secure messaging in general is summarized in [63]. There have also been a number of efforts toward creating self-destructing data, including early work by Perlman [52] and more recent work on Vanish [28, 29]. An analysis of different approaches for secure data deletion appears in [53]. There have also been significant efforts toward ephemeral and secure two-way communications, such as the off-the-record (OTR) messaging system [14, 32].

Though the above-mentioned technologies are valuable, our research suggests that many of them require steps or actions at odds with substantive aspects of the journalistic process or technical access issues of journalists and/or their sources. Moreover, these access issues are often most acute among the most vulnerable source populations with whom journalists work (e.g., sources involved in the criminal justice system).

Though some journalism-specific tools have been developed and deployed, notably SecureDrop [20, 26] and similar systems, our findings suggests that such anonymous document drops — while more secure — comprise only a small portion of journalists' source material. In a similar vein, Witness [7] and the Syria Accountability Project [59] focus on collecting and securely storing sensitive eyewitness data, but are not necessarily designed to protect the kind of ongoing communications that our research and other sources [37, 39] suggest commonly drives sensitive reporting.

3 Methodology

To make possible a sufficiently rigorous qualitative, grounded theory based [18, 30] analysis of the general and computer security needs and practices of journalists, we followed the recommendation of Guest et al. [35] to conduct 12-20 interviews, until new themes stopped emerging [18]. Our in-depth, semi-structured interviews were conducted with 15 journalists. Table 1 summarizes our participants and interviews.

Human subjects and ethics. Our study was approved by the human subjects review boards (IRBs) of our institutions before any research activities began. We obtained informed written or verbal consent from all participants, both to participate in the study as well as to have the interviews audio recorded. We transmitted and stored these audio files only in encrypted form. We did not record or store any explicitly identifying metadata (e.g., the name of a journalist or organization), nor do we report those here. Though we asked participants to reflect on recent source communications, including those that touched on sensitive information, we explicitly asked them *not* to reveal identifying information about specific sources or stories. As journalists are normally responsible for protecting source identities, these constraints were not out of the ordinary; indeed, we felt that the resulting interviews did not contain unnecessarily sensitive details.

3.1 Recruitment

We recruited our participants via our existing connections to journalistic institutions, usually via verbal or email contact with a staff member followed by an email containing our recruitment blurb. For better anonymity, participants at each organization were not recruited directly but were selected by our contact person according to individuals' availability at the time of the interviews. In communicating with the main organizational contacts, we stressed a desire for balance in terms of participants' technical skill and the sensitivity of their work. The vast majority of interviews were conducted in-person, though

a few were conducted via Skype.

For the purposes of this study, we limited our search for participants to journalists directly employed by well-respected journalistic institutions rather than freelance journalists. This focus allows us to explore the role of a journalist's employer in his or her computer security practices (or lack thereof). Our interviewees came from six different news organizations. Of these, four represent newsrooms and journalists who deal regularly with international (including non-Western) sources and stories of national and/or international profile. So while the organizations themselves are based in the U.S. and/or France, their work involves sources outside of those countries as well. The remaining organizations have a primarily U.S.-focused source base.

Nine interviews were conducted in France with journalists from French and U.S. journalistic institutions. Two of these interviews were conducted in French and were translated to English by another researcher. Both the interviewer and the translator are proficient in French. Due to our qualitative interview method and corresponding small sample size, we do not attempt to draw conclusions about differences between French and U.S. journalists in this work.

We do note that our participants are not necessarily representative of all journalists. It may be that journalists who agreed to speak with us are more (or less) security-conscious than those who declined, or that that the experiences of U.S. and French journalists differ from those of journalists in other countries. We also expect that the practices of freelance journalists differ from those of institutional journalists. Future work should study these questions; nevertheless, our interviews give us a valuable glimpse into the computer security practices and needs of a significant subset of the journalistic community.

3.2 Interview Procedure

One of the researchers conducted all of the interviews in the period from November 2014 through February 2015. Interviews were audio recorded and later transcribed and coded (more details below) by the remaining (non-interviewing) researchers. Each interview took between 15-45 minutes and had two parts:

Part 1: Questions about a specific story
We first prompted participants to tell us about the practices and tools that they use as journalists by asking them to think about a specific recent example. We asked:

> *Please think about a specific story that you have published in approximately the last year for which you spoke with a source. (There is no need to tell us the specific story or source, unless you believe this information is not sensitive and would like to share it.)*

In this context, we then asked about:

- Whether they had a relationship with the source prior to this story;
- How they first contacted the source about the story;
- Primary form(s) of communication with the source;
- Whether they would feel comfortable asking this source to use a specific communication method; and
- How representative this example is of their communication with sources in general.

Part 2: General questions
We then asked participants more general questions about their work as a journalist, including questions about:

- Their note-taking and storage process, and whether they take any steps to protect or share their notes;
- Problems that might arise if their digital notes or communications were revealed;
- Any non-technological strategies they use to protect themselves or their sources;
- Whether someone has ever recommended they use security-related technology in their work;
- How they define "sensitive" information or sources in their work;
- Any specific security-related problems to which they wish they had a solution;
- What kinds of devices they use, and who owns and/or administers them;
- Whether they have anyone, inside or outside of their organization, to whom they can go for help with computer security or other technologies; and
- Their self-described comfort level with technology and security-related technology.

Finally, we gave participants an opportunity to share any additional thoughts with us and to ask us any questions.

Throughout the interviews, we allowed participants to elaborate and ask clarification questions, and we asked follow-up questions where appropriate. As a result, the interviews did not necessarily proceed in the same order nor did they address identical questions.

3.3 Coding

To analyze the interviews, we used a grounded theory [18, 30] approach in which we developed a set of themes, or "codes", via an iterative process. After the interviewing researcher had conducted nearly half of the interviews, three additional researchers each independently listened to and transcribed several interviews. These researchers then met in person to develop, test, and iteratively modify an initial set of codes. Two researchers then independently coded each interview. As additional interviews were performed, the researchers reexamined and modified the codebook as necessary, going back and

		Participant		Interview			Technical Expertise	
Number	*Identifier*	*Gender*	*Organization (Type)*	*Location*	*Language*	*Length*	*General*	*Security*
1	P0	Male	Large, established	France	English	32 min	High	High
2	P1	Female	Large, new	USA	English	31 min	High	Medium
3	P2	Female	Large, established	France	English	39 min	Medium	Low
4	P3	Female	Large, established	France	English	39 min	High	Medium
5	P4	Female	Large, established	France	English	42 min	Medium	Low
6	P5	Male	Large, established	France	French	24 min	Medium	Low
7	P6	Male	Large, established	France	French	23 min	Medium	Medium
8	P7	Female	Large, established	France	English	27 min	High	Low
9	P8	Male	Large, established	France	English	20 min	High	Medium
10	P9	Male	Large, new	USA	English	41 min	High	Medium
11	P10	Female	Large, new	USA	English	31 min	Medium	Medium
12	P11	Female	Large, new	USA	English	19 min	Medium	Low
13	P12	Female	Small, new	USA	English	17 min	Medium	Low
14	P13	Female	Small, new	USA	English	34 min	High	Low
15	P14	Female	Small, established	USA	English	25 min	Medium	Medium

Table 1: **Interviews.** One researcher conducted all interviews between November 2014 and February 2015, at six well-respected journalistic institutions. The two interviews conducted in French were translated to English by another researcher (both researchers are proficient in French). On the right, we report participants' general and security-specific technical expertise; these values are self-reported. Organization size descriptors are based on those used by the Online News Association (`http://journalists.org/awards/online-journalism-awards-rules-eligibility/`). "New" organizations have existed for 10 years or less.

recoding previously coded interviews. This iterative process was repeated until the final codebook was created and all interviews were coded. The researchers then met in person to reach consensus where possible. We report inter-coder agreement inline with our results.

4 Results

We now turn to a discussion of results from our interviews. In designing and analyzing our interviews, we focused on several primary research questions, around which we organize this section:

1. What are the *general practices* of journalists in communicating with their sources?
2. What are the *security concerns* and threat models of journalists with respect to source communication?
3. What, if any, *defensive strategies* (technical or otherwise) do journalists employ to protect themselves or their sources? How and why do some possible defensive strategies succeed and others fail?
4. What are the *needs of journalists* in their communications with sources that are currently hampered or unfulfilled by computer security technologies?

By applying an appropriate qualitative analysis [18, 30, 35], we identify important themes and other observations present in the interviews. Where applicable, we report the raw number of participants who discussed a certain theme in order to give a rough indication of its prevalence amongst journalists. Our results are not quantitative, however: a given participant failing to mention a particular theme does not necessarily mean that it is inapplicable to him or her.

Each interview was coded independently by two researchers: a primary coder who coded all interviews, and two additional coders who coded non-overlapping sets of 9 and 6 interviews respectively. We report raw numbers based on the primary coder, with Cohen's kappa (κ) as a measure of inter-coder agreement [19] (averaging kappas for the two sets of coders). The average kappa for all results in the paper is 0.88. Fleiss rates any value of kappa over 0.75 as excellent agreement and between 0.40 and 0.75 as intermediate to good agreement [24].

4.1 Participants

Our participants are journalists working at major journalistic institutions in both the United States and France. Table 1 summarizes our 15 interviews and participants.

As reflected in Table 1, we spoke with journalists across the spectrum of general technical and computer security expertise. Some of our participants comfortably discussed their use of security tools such as encrypted chat and email, while others did not use or mention any security technologies at all. Regardless of technical and computer security expertise, our participants work with sources and stories of varying sensitivity. Stories considered "sensitive" by our participants include those involving information provided off-the-record by government officials, leaked or stolen documents, vulnerable populations (e.g., abuse victims or homeless people), and personal information that sources did not want published.

4.2 Key Findings

Before diving into our detailed results, we briefly highlight our key findings.

First, we find that journalist-source communications are often *driven by the source*. Participants tended to select communication mechanisms based on the comfort level, capacities, and preferences of sources, deferring to

them to specify the use of computer security tools rather than imposing these on sources. In this sense, the existing communication habits of sources are a primary obstacle to adoption of secure communication tools among journalists. In particular, the *digital divide*, in which source populations do not have access to or knowledge about technology, presents a serious challenge.

Additionally, our study reveals both *expected security concerns* (e.g., government surveillance, disciplinary consequences for sources) and *less expected security concerns* (e.g., financial impact on organizations) held by our participants. Participants described many *ad hoc defensive strategies* to address these concerns, including ways to authenticate sources, to obfuscate information in filenames and notes, and to obfuscate communications metadata by contacting sources through intermediaries.

Finally, beyond the expected *usability and adoption challenges* of computer security technologies, we find that a major barrier to adoption of these tools arises when they *interfere with a journalist's other professional needs*. For example, participants described the challenge of authenticating anonymous sources, and more generally, the need to reduce communication barriers with sources. Our study also reveals the need among journalists for a more general knowledge management platform, for which today's journalists use ad hoc methods based on tools like Google Docs and Evernote. This need may represent an opportunity to seamlessly integrate stronger computer security properties into journalistic practices.

4.3 General Practices

We begin by overviewing the general journalistic process described by our participants, in order to provide important context for the computer security community when it designs tools for journalists. We highlight security implications where applicable, and dive into these more deeply in later subsections.

Finding sources. Many participants discussed having long-term sources (10 of 15), particularly for sensitive information (e.g., sources in government). A different subset described finding new sources relevant to new stories (10 of 15), often by following referrals from previously known contacts. The importance of long-term sources poses security challenges: for example, it may be hard to protect metadata about communications over a long period, especially if the journalist's communication with that source is not always sensitive (and thus not always conducted over secure channels).

Communicating with sources. Our participants typically communicate with sources by email, phone, SMS, and/or in person. Security tools, such as encrypted messaging, were used only in exceptional cases where the context was known in advance to be sensitive, and both the journalist and source were sufficiently tech-savvy.

The choice of communication technology is typically determined by what is most convenient for the source, including the platform on which source is most likely to respond. Several participants discussed the importance of reducing communication barriers to sources. In the words of P13, *"taking down barriers is the most important thing to source communication."* Thus, if the source is concerned about security and sufficiently tech-savvy, the journalist may use security technologies to communicate; however, several of our participants expressed hesitation about interfering with a source's decision about what form of communication — even if insecure — is acceptable. For example, P9 said:

> *[The source] probably understand[s] the threat model they're under better than I would. So, it brings up an interesting question: do you go with what they're comfortable with? Or do you say, alright, actually let me assess what's going on and get back to you with what would be appropriate. [...] People's first impression is that they would go by what the source feels comfortable doing. As opposed to stepping in and being paternalistic about it.*

This finding suggests that the computer security community must consider sources as well as journalists when developing secure communication tools for journalism.

Building trust with sources. In order to feel comfortable providing sensitive information, a source must trust the journalist. While some trust with sources is built naturally over time, several participants mentioned explicit strategies for building trust with sources, including: speaking with people informally before they become official sources, being explicit with sources about what is "on the record," respecting sources' later requests not to include something in a story, and using security technologies to protect communications.

Communication tools. Table 2 summarizes the non-security-specific technologies participants mentioned using in their work. Primary communication tools include phone, SMS, and email, with limited use of social media to contact sources (usually as a last resort). In addition to digital communication, in-person meetings with sources are common. While some participants reported meeting in person for security reasons, most cited this as a means to gain higher quality information from sources.

Among storage technologies, we note that Google Docs/Drive is particularly popular, and that many of the tools mentioned involve syncing local data to cloud storage. Though cloud storage may have security implications (e.g., exposing sensitive data to third parties), few participants voiced these concerns explicitly.

Tool or technology	Number of participants (of 15)	Inter-coder agreement (κ)
Phone	15	1.00
Email (unencrypted)	15	1.00
Google Docs/Drive	8	1.00
Microsoft Word	8	1.00
SMS	8	1.00
Social media	7	0.83
Dropbox	4	1.00
Skype	4	1.00
Evernote	3	1.00
Text editor	2	1.00
Chat (unencrypted)	1	1.00
Scrivener	1	1.00

Table 2: **Non-security-specific tools.** This table reports the number of participants who mentioned using various non-security-specific tools or technologies in their work.

Devices and accounts. Though participants typically reported relatively strong "data hygiene" practices for email — i.e., conducting work-related communications only from a work email account — everyone we spoke to used at least one personal device or account for communicating with sources, including personal laptops and (more commonly) personal cell phones. Many participants reported using iPhones or iPads, often to take photos of documents or audio-record interviews. These devices are not necessarily encrypted, and the resulting files may be automatically backed up to cloud storage. Personal/professional distinctions were often blurred for social media accounts, and participants frequently reported using personal Google Drive, Dropbox, or Evernote accounts to sync, store and share data, particularly when the organization did not have its own enterprise Google Apps instance set up. As we discuss later, even participants who exhibited otherwise careful data security practices did not express concern about the security implications of storing data with third parties.

Many participants (7 of 15) reported that their employers have administrative access to their work computer, particularly at larger or older organizations. From a security perspective, this arrangement may allow organizations to ensure that journalists have updated systems and do not accidentally install malware, but it may also prevent journalists from installing security tools. It could also potentially expose sensitive information to the broader organization.

Two participants reported taking actions to circumvent the administrative rights of their employers: one insisted on being granted administrative access officially, while the other silently disabled his employer's remote access due to security and privacy concerns. He also mentioned being required to provide his laptop decryption key to his employer; he complied, but then re-encrypted his laptop and kept the new key to himself.

Note-taking. The journalists we spoke to described a variety of strategies for taking notes, most commonly audio-recording (13 of 15), electronic notes (12 of 15), and handwritten notes (10 of 15). We were somewhat surprised by the prevalence of audio recording, since such recordings may be particularly sensitive. Only two participants explicitly mentioned that they record audio only when intending to publish a full transcription.

We also asked participants about whether they share their notes with others. No one we spoke with ever shares notes outside of their organization, but many (13 of 15) sometimes share portions of notes within their organization. This sharing is typically done when working with another journalist on a story or for fact-checking. Most participants reported using some kind of third-party platform (e.g., Google Docs or Dropbox) for storing and sharing information. Several mentioned explicit strategies for sanitizing or redacting notes before sharing them (e.g., using codenames or omitting information); we discuss such strategies further in Section 4.5.

Knowledge management. We identify a possible opportunity for computer security in the knowledge management practices of journalists. In particular, several participants discussed strategies for organizing their notes and references for different projects and stories over time, including the use of file system folders, Google Drive, Evernote, and Scrivener. These knowledge management techniques were all ad hoc; no two participants described identical techniques. Indeed, several participants explicitly discussed the lack of a good knowledge management tool for journalists as a challenge. As we discuss in Section 4.6, this gap represents an opportunity for integrating computer security into the journalistic process.

4.4 Security Concerns

We now turn specifically to security-related issues, considering first the security concerns voiced in our interviews. Because one researcher's prior experience in the journalism community suggested that the term "threat modeling" is familiar but not widely understood, we elicited these concerns indirectly, by asking: "Of the information that you currently store digitally, would it be problematic if it were to become known to people or organizations outside of you and/or your news organization? If so, who would be at risk?" Because the concept of risk is dependent on a judgment about vulnerability, we also asked participants about their view on what kind of sources or information they considered "sensitive," whether or not they had worked with it personally.

Concrete threats experienced. A small number of participants reported encountering direct tangible threats or harms themselves in the course of their work. For example, one journalist told us that during his time report-

Category	Concern	Number of participants (of 15)	Inter-coder agreement (κ)
Threats to sources	Discovery by government	6	0.88
	Disciplinary action (e.g., lost job)	6	0.88
	Reputation/personal consequences	6	0.88
	Generally vulnerable populations (e.g., abuse victims)	4	0.65
	Discovery by others wishing to reveal identity	3	0.80
	Physical danger	3	0.86
	Prison	2	1.00
Threats to journalist or organization	Reputation consequences (incl. loss of source's trust)	9	0.89
	Being "scooped" (i.e., journalistic competition)	6	1.00
	False or misleading information from a source	4	0.36
	Physical threats (incl. theft)	2	0.50
	Financial consequences	1	1.00
Threats to others	Political / foreign relations consequences	1	0.50
	Other	1	1.00

Table 3: **Security concerns.** We report how many participants mentioned various threats to themselves, to their sources, to their organizations, or to others. These are not necessarily threats that participants have directly encountered or acted on themselves — that is, they discussed threats both in a hypothetical sense (concerns they have) and a concrete sense (real issues they have encountered).

ing on government-related scandals, his work phones had been wiretapped, his laptop (and nothing else) had been stolen from his home, and he had received letters threatening his and his family's lives and safety. Another described communications with contacts in a foreign region, in which phone communications were regularly terminated when the conversation broached what she perceived as sensitive topics. In total, 6 participants mentioned the knowledge or strong suspicion that their or their sources' digital communications had been retroactively collected or actively monitored.

General concerns. In addition to these concrete attacks and threats, participants mentioned a range of risks that they consider in communications with sources. These concerns are organized and summarized in Table 3.

Many of the general security concerns reported by participants were in line with our expectations: governments attempting to identify sources, reputational threats or harms, and legal or disciplinary consequences. The most common concern involved reputational harm and loss of credibility by the journalist and his or her organization, largely characterized as a compromised ability to gain access to and establish trust with future sources.

Participants also mentioned several threats that we had not initially anticipated. For example, one participant discussed the possible financial consequences to his organization when it reported on a scandal involving a major advertiser. Several participants mentioned concern about being "scooped" by other journalists if they lost their competitive advantage in having early access to certain information. One participant worried that her web searches on sensitive work-related topics would make her a surveillance target in her personal life, so she avoided doing those searches on her home computer.

Overlooked concerns. We identify several security concerns that were generally overlooked by our participants, despite being well-known to computer security experts.

Third parties. Only one participant expressed concern about the trustworthiness of major third parties, such as Apple, Google, or Microsoft. While some participants expressed hesitation about how secure a certain practice is, they did not explicitly discuss these major technology providers as being a possible security risk. Unfortunately, this implicit trust assumption may not be warranted — e.g., consider reports of government or other compromises of major companies [34, 66] and the FBI's National Security Letters compelling service providers to release information [50].

Metadata. While a few participants expressed concerns about the metadata connecting them to their sources (discussed further in Section 4.5 below), most did not discuss metadata as a threat even implicitly. Indeed, even those who explicitly took steps to protect their notes or communications (e.g., using encryption) did not generally discuss the need to similarly protect metadata.

Legal concerns. Finally, there was virtually no mention in any of the interviews of the risk of lawsuit resulting from or discovery of digitally stored or communicated information. There are several possible explanations for this, though comments from most of those interviewed suggest that they did not feel their own work was ever likely to be the subject of a government investigation.

4.5 Defensive Strategies

Whether or not they had experienced concrete threats, most participants reported using some defensive strategies, including security technologies as well as non-technical or technology-avoidant strategies. Figure 4 systematizes these strategies, and Table 5 summarizes participants' use of specific security technologies.

Category	Defense	Number of participants (of 15)	Inter-coder agreement (κ)
Technical defenses	Encrypting digital notes	6	1.00
	Keeping files local (not in the cloud)	5	0.89
	Encrypted communication with colleagues	3	0.81
	Circumventing organization's admin rights on computer	2	0.50
	Encrypted communication with sources	2	0.50
	Anonymous communication (e.g., over Tor)	2	1.00
	Air-gapping a computer (keeping it off the internet)	1	1.00
	Using additional, secret devices or temporary burner phones	1	1.00
	Visually obscuring information in photos/videos (e.g., blurring)	1	0.50
Ad hoc non-technical strategies	Using code names in communications or notes	8	1.00
	Claiming bad handwriting as a defense for written notes	3	1.00
	Contacting sources through intermediaries	2	0.81
	Citing multiple sources to create plausible deniability	1	1.00
	Using some method to authenticate source	1	1.00
Explicitly avoiding technology	Communicating in person	7	0.72
	Self-censoring (avoiding saying things in notes/email)	6	0.86
	Communicating only vague information electronically	5	0.83
	Physically mailing digital data (e.g., on USB stick)	2	1.00
Physical defenses	Home alarm system	1	1.00
	Physical safe (e.g., to store notes)	1	1.00
	Shredding paper documents	1	1.00

Table 4: **Defensive techniques.** We report the number of participants who mentioned using various defensive techniques to protect themselves, their notes, and/or their sources.

	Number of participants (of 15)				Inter-coder
Security tool or technology	*Use regularly*	*Tried but don't use*	*Haven't tried*	*Not mentioned*	**agreement (κ)**
Dispatch	0	0	1	14	1.00
Encrypted chat (e.g., OTR, CryptoCat)	5	0	1	9	0.90
Encrypted email (e.g., GPG, Mailvelope)	4	4	1	6	0.92
Encrypted messaging (e.g., Wickr, Telegram)	0	1	0	14	1.00
Encrypted phone (e.g., SilentCircle)	0	2	0	13	1.00
Other encryption (e.g., hard drive, cloud)	5	1	0	9	1.00
Password manager	1	0	1	13	1.00
SecureDrop	0	0	1	14	1.00
Tor	2	1	0	12	0.89
VPN	2	1	0	12	1.00

Table 5: **Security tools.** This table lists security technologies discussed by participants. We report on the number who regularly use, have tried but don't regularly use, and haven't tried each tool. We consider use to be "regular" even if it depends on the sensitivity of the source or story, i.e., if the journalist regularly employs that tool when appropriate, even if not in every communication.

Non-technical defensive strategies. Since not all of our participants were computer security experts — and certainly most journalists are not — we were particularly interested in non-technical or otherwise ad hoc strategies that they have developed to protect themselves, their notes, or their sources. As reflected in Table 4, a commonly mentioned non-technical strategy is avoiding technology entirely, e.g., meeting sources face-to-face, physically mailing digital data, and/or communicating only vague information electronically. For example, P6 told us (translated from French):

> *I don't use phones, I don't send email. Sometimes I send SMS messages, but these messages are very vague.* [Later in the interview he adds:] *I don't use technical methods [to protect my sources]. I prefer to work in an old fashioned way. A little bit like Bin Laden did.*

The reference to Bin Laden echoes an issue raised in a recent report about U.S. journalists, which describes how concerns about surveillance and increased leak investigations have caused journalists to feel like they must "act like criminals" to communicate with sources [40].

Some of these non-technical strategies, however, were cited specifically for their journalistic rather than their security value. In explaining the choice to meet a source primarily in person, participant P11 noted:

> *I think it's always preferable because of the level of intimacy and information that you gain. You get better results and [...] you can sort of verify in different ways the stories that they're telling you.*

Ad hoc defensive strategies. We also uncovered a number of ad hoc strategies that make incidental use of tech-

nology. For example, participant P0 described his strategy for authenticating a source whose email address he found on a public mailing list: he asked that source to post a particular sentence on Twitter, allowing P0 to verify that the email and Twitter accounts indeed belonged to the same individual. In another example, P5 described a strategy for hiding the connection between himself and a sensitive source in the government by contacting the source through an intermediary. In particular, P5 called the source's assistant at previous job and stated a false name; when the assistant passed this message on, the source knew whom to contact.

These strategies of avoiding technology entirely or using ad hoc methods for specific cases suggest that our participants (and/or their sources) are not always comfortable with existing security technologies, and/or that these technologies do not meet their security needs in a straightforward way, as we discuss further in Section 4.6.

Technical defensive strategies. As reflected in Table 4, several participants explicitly mentioned using security technologies to protect themselves, their notes, or their sources. Table 5 summarizes specific security technologies mentioned, broken down by how often participants mentioned using these technologies.

Most commonly, participants mentioned using encryption to protect communications or stored data. Even participants with low computer security expertise often mentioned and even used encryption. For example, P5, who otherwise mentioned no technical security strategies, uses the Mac Disk Utility to encrypt virtual drives on his machine. Indeed, several participants mentioned using built-in file or disk encryption of this sort, suggesting that these tools are reasonably discoverable and usable. The lack of installation overhead may also contribute to their prevalence among our participants.

Participants who reported use of computer security technology for source communication fell roughly into two groups: those whose sources demanded it, and those who had participated in some kind of computer security training either through their workplace or at an external event. Sustained use, however, was seen only in intra-institutional communications (largely chat). Those who used these tools for communication with sources did so only sporadically (as required by a particular source), and reported an extended timeframe to become comfortable using them (particularly GPG and OTR).

We observe several security technologies that were under-represented in our interviews. For example, SecureDrop [26] and Dispatch [12], which were designed specifically for journalists, were mentioned by only one participant who did not report ever having used them.

Reasons for not using security technologies. We asked participants whether anyone (a source, a colleague, or anyone else) had ever recommended that they use any computer security tools or technologies. Of our 15 participants, 10 replied that they had received such a recommendation. Of those, however, only four began regularly using any of the recommended tools.

For participants who had never tried, or tried but did not continue using tools mentioned in the interview (see Table 5), we coded the interviews for reasons for not using security technologies. These reasons are summarized in Table 6, and we highlight a few important issues here.

Usability, reliability, and education. Echoing findings from prior studies (e.g., [65]), many participants discussed challenges related to usability of security tools and the need for education of journalists and sources about security issues. These challenges result in limited adoption of these tools among sources and colleagues, reducing their utility to even the most technically savvy journalist. For example, one participant described a situation where he and his colleagues worked with sensitive data; as the size of the group grew and included less security-versed individuals, it became harder to maintain strict data security practices (echoing prior findings about the social context surrounding such tools [27]).

In addition to the well-known usability challenges with many security tools, participant P10 described the difficulty of knowing which tools to trust:

> *A lot of services out there say they're secure, but having to know which ones are actually audited and approved by security professionals — it takes a lot of work to find that out.*

Digital divide. A challenge frequently mentioned in our interviews (by 4 of 15 participants) is the "digital divide": many sources do not understand or even have access to computer security technology, making it infeasible for journalists to use technical tools to secure their communications with these sources. As our participants described, this challenge applies particularly to vulnerable populations, such as low-income communities, abuse victims, homeless people, etc. To take just one example, P12 discussed the digital divide as follows:

> *Most of the [sensitive sources] I've worked with [are] also people who probably aren't very tech-savvy. Like, entry-level people in prisons, or something like that. So if they were really concerned about communication, I don't quite know what a secure, non-intimidatingly-techy way would be. [...] Some of them don't even necessarily have email addresses.*

Lack of institutional support for computer security. Another important challenge for some journalists attempting to use security technologies is a lack of institutional support. Though some participants described supportive organizations, 9 of 15 mentioned that they did *not* have

Category	Reasons for not using security technology	Number of participants (of 15)	Inter-coder agreement (κ)
Usability and adoption	Not enough people using it	5	0.79
	Digital divide: sources don't have/understand technology	4	0.86
	Security technology is too complicated	3	1.00
	Hard to evaluate credibility/security of a tool	2	0.50
Interference with journalism	Creates barrier to communication with sources	5	0.64
	Doesn't want to impose on sources	5	0.83
	Interferes with some other part of their work	3	1.00
Other	Work isn't sensitive enough / no one is looking	8	0.41
	Uses a non-technical strategy instead	6	0.70
	Insufficient support from organization	2	0.80
	Tool doesn't provide the needed defense	1	1.00

Table 6: **Reasons journalists report not using security technologies.** We report the number of participants who mentioned various reasons for why they haven't tried or don't regularly use computer security technologies. Note that some of these themes may overlap (i.e., a single statement made by a participant may have been coded with more than one of the themes in this table).

anyone to go to for help with computer security issues who was both within their organization and whose role explicitly involved providing technical support of this nature. Instead, 5 participants had no one to ask for help or had to go outside their organizations, while 4 received help from other journalists within their organization who happened to be knowledgable about these issues (e.g., because they cover related stories). Similarly, many participants (6 of 15) explicitly reported not having administrative privileges on their work computers, making it difficult or impossible to install security tools not officially supported by the organizations.

Inconsistencies and vulnerabilities. Finally, we reflect on several inconsistencies or vulnerabilities that we observed in the described behaviors of our participants.

A common inconsistency (observed in 5 of 15 interviews) involved protecting data effectively in one context but insufficiently in another. For example, participant P5 (quoted above) avoids using technology to communicate with sources due to real threats he has encountered (including eavesdropping, laptop theft, and death threats) — but uses his iPad (with no mention of encryption) to photograph sensitive documents provided without permission by sources.

Participants also frequently discussed or acknowledged the potential danger in a particular practice, but did not change their behavior. For example, P10 told us: *"I should have a separate work [Gmail] account but I just use my personal one"* — a sentiment echoed by other participants. As another example, when asked if he takes steps to protect his notes, P5 responded: *"I should. But no."* In another case, though a participant considered herself "comfortable" with computer security technology and worked with sensitive information, she did not use and seemingly could not name any security tools.

We also identified several vulnerabilities present in the behaviors of participants but not explicitly acknowledged by any of them. For example, while some participants explicitly mentioned meeting with sources face-to-face for security reasons (in addition to journalistic reasons), they did not mention taking precautions like leaving behind or turning off electronic devices at these meetings. Indeed, many participants (though not necessarily those using face-to-face meetings for security reasons) mentioned using their iPhones or other devices to audio-record in-person conversations with sources. Participants also frequently use document management services that sync data to a third-party cloud service, such as Google Docs and Evernote.

4.6 Needs of Journalists

A major goal of our study is to inform future efforts by the computer security community to develop tools to protect journalist-source communications. To that end, we identify needs of journalists in their communications with sources that are hampered or unfulfilled by current computer security technologies. Needs that are still unfulfilled present immediate opportunities for future work, while needs that are hampered suggest reasons why existing technologies have failed to find greater adoption.

Functions impeded by security technology. One of the reasons that participants noted for why they have not tried or do not regularly use certain security technologies is that they interfere with some component of the journalistic process. As reflected in Table 6, 3 of 15 participants mentioned this reason. Taking a closer look at which functions are impeded by existing security technologies (and should be considered in future tools for journalists), our participants mentioned the following problems:

- Anonymous communications may make it difficult for journalists to authenticate sources, or to authenticate themselves to sources.
- Using security tools may impede communications with colleagues who don't use or understand them.
- Constraints on communications with sources may reduce the quality of information journalists can get.

For example, P13 described the tension between anonymous sources and authenticity:

> *If I don't know who they are and can't check their background, I'm not going to use the information they give. Anonymous sourcing is fine if I know who they are, and I've checked who they are, and my editor knows who they are, but they can't keep that from me and then expect me to use the information they provide.*

In other words, a source's communications must be anonymous to everyone but the journalist with whom they are communicating, and that journalist must be able to prove the authenticity of that source to others (e.g., their editor). This need suggests that tools like SecureDrop [26], which supports anonymous document drops for journalists, are unlikely to be widely adopted in isolation — highlighting the need for the computer security community to interface with the journalism community.

On the flip side, P6 discussed the need for sources to authenticate him when he attempts to reach them, describing how sources are unlikely to answer the phone if they cannot see who is calling them.

In order to develop computer security technologies that will be widely adopted by journalists, the computer security community must understand such failures of existing tools. We emphasize that these failures are not merely the result of computer security tools being hard to use (a common culprit [65]) but often arise when a tool did not sufficiently account for functions important in a journalist's process, such as the ability to authenticate sources. In Section 5, we discuss what the specific failures above mean for where technologists should focus their efforts in this space.

Security needs unfulfilled by technology. In the previous paragraphs, we described needs of journalists that we infer from their reasons for not using certain security technologies. In addition to making these inferences, we also asked participants to report specifically on any concerns or issues related to computer security to which they have not yet found a good technical solutions (i.e., "I wish somebody would build a tool that does X"). From the responses to this question, we extract several technical security-related needs currently unaddressed.

Usability, education, and adoption. As discussed above, several participants mentioned usability concerns (the need for more usable security tools) and education concerns (the need for education about these issues for both sources and journalists), both for themselves and to increase the adoption of security technologies among others. Specifically, participants asked for better and easier-to-use tools or services for encrypted email, encrypted file sharing, and encrypted phone calls, as well as ways to prevent emails from being accidentally forwarded and to keep sensitive data off the Internet (e.g., air-gapping).

Mutual authentication and first contact. Some participants discussed ad hoc strategies to authenticate sources, or to authenticate themselves to sources. As noted above, current security tools for journalists may hamper these needs, rather than addressing them. Participant P0 spoke in particular about the tension between anonymity and authentication in first contact:

> *The first contact is never or very rarely anonymous or protected. If someone wants to give me some information and we don't already know each other, how would he do it? He could send me an email, yeah, okay — but then how could I be sure it's him? Unless he contacts me with his real identity first. It's very difficult to have the first contact secure.*

In this "first contact" problem, it is nearly impossible for journalists to entirely avoid *some* metadata trail when communicating with a source, since their initial contact will almost universally take place over a channel whose metadata is associated with the journalist's professional identity (e.g. telephone, email, or social media). Given the pivotal role that metadata has played in recent leak prosecutions [54], this is a significant security concern.

Digital divide. As discussed above, several participants expressed the need for better security technologies that work across the digital divide, in order to protect their communications with sources who have low technical expertise and/or limited access to technology.

These unfulfilled needs represent immediate opportunities for future work on secure journalist-source communications within the computer security community, with varying types and degrees of challenge. We discuss these new directions further in Section 5.

Other technical needs. Though we asked participants specifically about unaddressed issues related to computer security, a few also (or instead) expressed more general technical needs that have security implications.

For example, several participants discussed the difficulty of manually transcribing audio recordings of interviews and expressed a desire for better machine transcription. Our interviews show this unaddressed need led to at least one insecure practice by a participant, who described planning to use her iPhone's or Mac's speech-to-text feature to transcribe audio recordings of interviews with sources, seemingly unaware that this might send the audio of potentially sensitive interviews to the cloud [9]. Thus, as journalists develop ad hoc workarounds for tasks where a technical solution is missing from their toolset, they may unintentionally introduce vulnerabilities into their process.

More generally, as mentioned above, several partic-

ipants discussed the need for a systematic knowledge management tool for journalists. P11 was most explicit:

> *There were different kinds of litigation software that I was familiar with as a lawyer, where, let's say, you have a massive case, where you have a document dump that has 15,000 documents. [...] There are programs that help you consolidate and put them into a secure database. So it's searchable [and provides a secure place where you can see everything related to a story at once]. I don't know of anything like that for journalism.*

This absence of a dedicated knowledge management tool for journalists represents an opportunity for computer security. If such a knowledge management tool seamlessly integrated computer security techniques to protect stored data and communications without significant effort on the part of the journalist, it would significantly raise the bar for the security of journalist-source communications.

5 Discussion

We elaborate on the implications of our findings for the computer security community and make concrete recommendations for how those considering journalist-source communications can most fruitfully direct their efforts.

5.1 Key Take-Aways

From the perspective of the computer security community, we consider the following take-aways to be the most important ones from our findings:

- Journalists commonly make decisions about how to communicate with sources based on the technical access and comfort level of the sources themselves. Thus, limited adoption of technical security tools for journalist-source communications stems in large part from the limited technical access and expertise of certain vulnerable populations.
- Journalists face technical challenges unrelated to computer security, including the lack of systematic knowledge management tools and limited technical support for transcription. In developing ad hoc strategies to deal with these challenges, journalists sometimes introduce additional security vulnerabilities into their practices.
- A journalist's organization plays an important role in his or her access to and competence with computer security technologies. Organizations that restrict a journalist's ability to install security (or other software) tools, or where many employees have limited technical expertise, reduce the effectiveness and adoption of security and other technologies.
- An important reason for the failure of some security tools in the journalistic context is their incompatibility with some essential aspect of the journalistic process. A tool that increases barriers to communication or prevents a journalist from determining the authenticity of a source will see limited adoption.

5.2 Recommendations

In addition to supporting ongoing efforts at educating and training journalists with respect to existing computer security technologies (e.g., [17, 43, 47, 62]), we distill from our findings the following recommendations for where the computer security community should focus its efforts.

First contact and authentication. The challenge of securing (or retroactively protecting) a journalist's first contact with a source remains a hard problem, especially given the tension between anonymity and mutual authentication. Determining authenticity, both of sources and of journalists, is of fundamental importance in the journalistic context and should be addressed explicitly by anonymous communication tools. For instance, successful approaches might leverage existing identity networks, as with the participant who asked his source to post a specific sentence on Twitter — similar to social authenticity proofs used by Keybase (`https://keybase.io/`).

Metadata protection. Protecting metadata of journalist-source communications is crucial, especially in light of successful leak prosecutions based on metadata information [54]. In practice, metadata is both legally and technically unprotected: none of the defensive strategies described by our participants was truly foolproof, especially with respect to metadata. Protecting metadata is challenging because it requires that both journalists and sources understand the risk, because it is brittle (e.g., a single failure to communicate securely can compromise dozens or hundreds of exchanges), and because it can conflict with other journalistic needs (e.g., the need for authentication in first contact). The computer security community should consider metadata protection in this context and develop effective, usable, and transparent solutions that can account for long-term communications of varying sensitivity.

Focus on sources. Since the methods and security of journalist-source communications often depend on the technical expertise and access of sources, the computer security community should focus not only on educating and building tools for journalists but also for sources. Enabling and improving access to computer security technologies for low-income and vulnerable populations (e.g., through a collaboration with public libraries and/or by supporting "dumb" phones or other access methods) will provide benefits to these communities far beyond their interaction with journalists. Meanwhile, future

studies should also interview and/or survey sources to shed light on their perspectives and needs.

Knowledge management. Our findings suggest that journalists desire — but lack — a solution for systematic knowledge management to support storing, organizing, searching, and indexing story-related data and documents. This need presents an opportunity for computer security: if security techniques and tools are seamlessly and usably integrated into a well-designed knowledge management tool for journalists, these could see wide adoption within the industry and significantly raise the bar for the security of journalistic practices. For example, given the reliance among our interviewees on third-party cloud storage, a secure (and easy-to-use) cloud storage solution integrated into such a knowledge management tool would provide significant benefits. A knowledge management tool that also supports secure communication — such as encrypted chat or email within the organization — would also benefit affiliated but non-staff members of the organization (e.g., freelancers).

Understanding the journalistic process. We encourage the technical computer security community to continue engaging closely with the journalism community. While many of the themes observed in our interviews and highlighted in this paper may be well-known within the journalism community, several of them were surprising to us. The prevalence of ad hoc defensive strategies among our participants suggests mismatches between existing computer security tools and the needs and understandings of journalists. To create technical designs that address journalists' most significant security problems without compromising necessary professional practices, the computer security community must develop a deep understanding of the journalistic process. These efforts are likely to be most valuable if they are iterative, involving the development of tools that are then evaluated and refined in the field among the target population.

Broader applicability. Finally, successful techniques for securing journalist-source communications are likely to apply to — or provide lessons for — other contexts as well, such as communications between lawyers and their clients, between doctors and patients, in government operations, among dissidents and activists, and for other everyday users of technology.

6 Conclusion

Though journalists are often considered likely users and beneficiaries of secure communication and data storage tools, their practices have not been been studied in depth by the academic computer security community. To close this gap and to inform ongoing and future work on computer security for journalists, we conducted an in-depth, qualitative study of 15 journalists at well-respected journalistic institutions in the U.S. and France.

Our findings provide insight into the general journalistic practices and specific security concerns of journalists, as well as the successes and failures of existing security technologies within the journalistic context. Perhaps most importantly, we find that existing security tools have seen limited adoption not just due to usability issues (a common culprit) but because of a mismatch between between the assumed and actual practices, priorities, and constraints of journalists. This mismatch suggests that secure journalistic practices depend on a meaningful collaboration between the computer security and the journalism communities; we take an important step towards such a collaboration in this work.

Acknowledgements

We gratefully acknowledge our anonymous reviewers for their helpful feedback. We also thank Greg Akselrod and Kelly Caine for valuable discussions; Raymong Cheng, Roxana Geambasu, Tadayoshi Kohno, and Sam Sudar for feedback on earlier drafts; and Tamara Denning for guidance on interview coding. Most importantly, we thank our interviewees very much for their participation in our study. This research is supported in part by NSF Award CNS-1463968.

References

[1] CCleaner. http://ccleaner.en.softonic.com/.

[2] Cryptocat: Chat with privacy. https://crypto.cat/.

[3] Silent Circle. https://silentcircle.com/.

[4] Tails: The Amnesic Incognito Live System. https://tails.boum.org/.

[5] TrueCrypt. http://truecrypt.sourceforge.net/.

[6] Wickr. https://wickr.com/.

[7] WITNESS, 2014. http://witness.org.

[8] APPLE. FileVault. http://support.apple.com/kb/ht4790.

[9] APPLE. OS X Mavericks: Use Dictation to create messages and documents, May 2014. http://support.apple.com/kb/PH14361.

[10] ARDAGNA, C. A., JAJODIA, S., SAMARATI, P., AND STAVROU, A. Providing Mobile Users' Anonymity in Hybrid Networks. In *European Symposium on Research in Computer Security (ESORICS)* (2010).

[11] BALL, J. GCHQ captured emails of journalists from top international media. The Guardian, Jan. 2015. http://www.theguardian.com/uk-news/2015/jan/19/gchq-intercepted-emails-journalists-ny-times-bbc-guardian-le-monde-reuters-nbc-washington-post.

[12] BISCUITWALA, K., BULT, W., MATHIAS LECUYER, T. J. P., ROSS, M. K. B., CHAINTREAU, A., HASEMAN, C., LAM, M. S., AND MCGREGOR, S. E. Secure, Resilient Mobile Reporting. In *Proceedings of ACM SIGCOMM* (2013).

[13] BLOND, S. L., URITESC, A., GILBERT, C., CHUA, Z. L., SAXENA, P., AND KIRDA, E. A look at targeted attacks through the lense of an ngo. In *23rd USENIX Security Symposium* (2014).

[14] BORISOV, N., GOLDBERG, I., AND BREWER, E. Off-the-record communication, or, why not to use PGP. In *Proceedings of the ACM Workshop on Privacy in the Electronic Society* (2004).

[15] BRENNAN, M., METZROTH, K., AND STAFFORD, R. Building Effective Internet Freedom Tools: Needfinding with the Tibetan Exile Community. In *7th Workshop on Hot Topics in Privacy Enhancing Technologies (HotPETs)* (2014).

[16] BUMP, P. So, You Want to Hide from the NSA? Your Guide to the Nearly Impossible. The Wire, July 2013. http://www.thewire.com/technology/2013/07/so-you-want-hide-nsa-your-guide-nearly-impossible/66942/.

[17] CARLO, S., AND KAMPHUIS, A. Information Security for Journalists. The Centre for Investigative Journalism, July 2014. http://www.tcij.org/resources/handbooks/infosec.

[18] CHARMAZ, K. *Constructing Grounded Theory*, second ed. SAGE Publications Ltd, 2014.

[19] COHEN, J. A Coefficient of Agreement for Nominal Scales. *Educational and Psychological Measurement 20*, 1 (1960), 37.

[20] CZESKIS, A., MAH, D., SANDOVAL, O., SMITH, I., KOSCHER, K., APPELBAUM, J., KOHNO, T., AND SCHNEIER, B. DeadDrop/StrongBox Security Assessment. Tech. Rep. UW-CSE-13-08-02, Department of Computer Science and Engineering, University of Washington, 2013.

[21] DANEZIS, G., AND DIAZ, C. A survey of anonymous communication channels. Tech. Rep. MSR-TR-2008-35, Microsoft Research, January 2008.

[22] DINGLEDINE, R., MATHEWSON, N., AND SYVERSON, P. Tor: The second-generation onion router. In *Proceedings of the 13th USENIX Security Symposium* (2004).

[23] EDMAN, M., AND YENER, B. On anonymity in an electronic society: A survey of anonymous communication systems. *ACM Computing Surveys 42*, 1 (2009).

[24] FLEISS, J. L., LEVIN, B., AND PAIK, M. C. *Statistical Methods for Rates and Proportions*, 3 ed. John Wiley & Sons, New York, 2003.

[25] FRANCESCHI-BICCHIERAI, L. Meet the Man Hired to Make Sure the Snowden Docs Aren't Hacked. Mashable, May 2014. http://mashable.com/2014/05/27/micah-lee-greenwald-snowden/.

[26] FREEDOM OF THE PRESS FOUNDATION. SecureDrop (formerly known as DeadDrop, originally developed by Aaron Swartz), 2013. https://pressfreedomfoundation.org/securedrop.

[27] GAW, S., FELTEN, E. W., AND FERNANDEZ-KELLY, P. Secrecy, flagging, and paranoia: Adoption criteria in encrypted e-mail. In *Proceedings of CHI* (2006).

[28] GEAMBASU, R., KOHNO, T., KRISHNAMURTHY, A., LEVY, A., LEVY, H. M., GARDNER, P., AND MOSCARITOLO, V. New directions for self-destructing data. Tech. Rep. UW-CSE-11-08-01, University of Washington, 2011.

[29] GEAMBASU, R., KOHNO, T., LEVY, A., AND LEVY, H. M. Vanish: Increasing Data Privacy with Self-Destructing Data. In *Proceedings of the 18th USENIX Security Symposium* (2009).

[30] GLASER, B. G., AND STRAUSS, A. L. *The Discovery of Grounded Theory: Strategies for Qualitative Research*. Aldine Publishing Company, Chicago, 1967.

[31] GNUPG. GNU Privacy Guard. https://www.gnupg.org/.

[32] GOLDBERG, I. Off-the-record messaging. https://otr.cypherpunks.ca/.

[33] GREENBERG, A. Whistleblowers Beware: Apps Like Whisper and Secret Will Rat You Out. Wired, May 2014. http://www.wired.com/2014/05/whistleblowers-beware/.

[34] GREENWALD, G. *No Place To Hide: Edward Snowden, the NSA, and the U.S. Surveillance State*. Metropolitan Books, 2014.

[35] GUEST, G., BUNCE, A., AND JOHNSON, L. How many interviews are enough? an experiment with data saturation and variability. *Field Methods 18*, 1 (2006).

[36] HARDY, S., CRETE-NISHIHATA, M., KLEEMOLA, K., SENFT, A., SONNE, B., WISEMAN, G., GILL, P., AND DEIBERT, R. J. Targeted threat index: Characterizing and quantifying politically-motivated targeted malware. In *23rd USENIX Security Symposium* (2014).

[37] HENINGER, N., POITRAS, L., GILLUM, J., AND ANGWIN, J. How Journalists Use Crypto To Protect Sources. Panel Discussion at 31th Chaos Communication Congress (31c3) of the Chaos Computer Club (CCC), Jan. 2015. https://www.youtube.com/watch?v=aviUKt7adU8.

[38] HILL, K. Lavabit's Ladar Levison: 'If You Knew What I Know About Email, You Might Not Use It'. Forbes, Aug. 2013. http://www.forbes.com/sites/kashmirhill/2013/08/09/lavabits-ladar-levison-if-you-knew-what-i-know-about-email-you-might-not-use-it/.

[39] HOLMES, H., MOSER, A., AND GELLMAN, B. Drop It Like It's Hot: Secure Sharing and Radical OpSec for Investigative Journalists. Panel Discussion at Hope X, July 2014. http://www.hope.net/schedule.html#dropitlike.

[40] HUMAN RIGHTS WATCH. With Liberty to Monitor All: How Large-Scale US Surveillance is Harming Journalism, Law, and American Democracy, July 2014. http://www.hrw.org/node/127364.

[41] HUNTLEY, S., AND MARQUIS-BOIRE, M. Tomorrow's News is Today's Intel: Journalists as Targets and Compromise Vectors. BlackHat Asia, Mar. 2014. https://www.blackhat.com/docs/asia-14/materials/Huntley/BH_Asia_2014_Boire_Huntley.pdf.

[42] INTERNEWS CENTER FOR INNOVATION & LEARNING. Digital Security and Journalists: A SnapShot of Awareness and Practices in Pakistan, May 2012. https://www.internews.org/sites/default/files/resources/Internews_PK_Secure_Journalist_2012-08.pdf.

[43] LEE, M. Encryption Works: How to Protect Your Privacy in the Age of NSA Surveillance. Freedom of the Press Foundation, July 2013. https://pressfreedomfoundation.org/sites/default/files/encryption_works.pdf.

[44] LEVISON, L. Lavabit, 2004. http://lavabit.com/.

[45] MARCZAK, W. R., SCOTT-RAILTON, J., MARQUIS-BOIRE, M., AND PAXSON, V. When governments hack opponents: A look at actors and technology. In *23rd USENIX Security Symposium* (2014).

[46] MARIMOW, A. E. Justice Departments scrutiny of Fox News reporter James Rosen in leak case draws fire. The Washington Post, May 2013. http://www.washingtonpost.com/local/justice-departments-scrutiny-of-fox-news-reporter-james-rosen-in-leak-case-draws-fire/2013/05/20/c6289eba-c162-11e2-8bd8-2788030e6b44_story.html.

[47] MCGREGOR, S. E. Digital Security and Source Protection for Journalists. Tow Center for Digital Journalism, July 2014. http://towcenter.org/blog/digital-security-and-source-protection-for-journalists/.

[48] MITCHELL, A., HOLCOMB, J., AND PURCELL, K. Investigative journalists and digital security: Perceptions of vulnerability and changes in behavior. Pew Research Center, Feb. 2015. http://www.journalism.org/files/2015/02/PJ_InvestigativeJournalists_0205152.pdf.

[49] NORCIE, G., BLYTHE, J., CAINE, K., AND CAMP, L. J. Why Johnny Can't Blow the Whistle: Identifying and Reducing Usability Issues in Anonymity Systems. In *Proceedings of the Network and Distributed System Security Symposium (NDSS) Workshop on Usable Security (USEC)* (2014).

[50] OFFICE OF THE INSPECTOR GENERAL. A Review of the Federal Bureau of Investigation's Use of National Security Letters. U.S. Department of Justice, Aug. 2014. http://www.justice.gov/oig/reports/2014/s1408.pdf.

[51] OLSON, P. E-mail's Big Privacy Problem: Q&A With Silent Circle Co-Founder Phil Zimmermann, Aug. 2013. http://www.forbes.com/sites/parmyolson/2013/08/09/e-mails-big-privacy-problem-qa-with-silent-circle-co-founder-phil-zimmermann/.

[52] PERLMAN, R. The ephemerizer: Making data disappear. *Journal of Information System Security 1* (2005), 51–68.

[53] REARDON, J., BASIN, D., AND CAPKUN, S. SoK: Secure Data Deletion. In *Proceedings of the IEEE Symposium on Security and Privacy* (2013).

[54] SAVAGE, C. Court Rejects Appeal Bid by Writer in Leak Case. The New York Times, Oct. 2013. http://www.nytimes.com/2013/10/16/us/court-rejects-appeal-bid-by-writer-in-leak-case.html.

[55] SAVAGE, C., AND KAUFMAN, L. Phone Records of Journalists Seized by U.S. The New York Times, May 2013. http://www.nytimes.com/2013/05/14/us/phone-records-of-journalists-of-the-associated-press-seized-by-us.html.

[56] SCHAFFER, M. Who Can View My Snaps and Stories, Oct. 2013. http://blog.snapchat.com/post/64036804085/who-can-view-my-snaps-and-stories.

[57] SECONDMUSE. Information Security for Journalists, June 2014. https://speakerdeck.com/secondmuse/understanding-internet-freedom-vietnams-digital-activists.

[58] SIERRA, J. L. Digital and Mobile Security for Mexican Journalists and Bloggers. Freedom House, 2013. http://www.freedomhouse.org/report/special-reports/digital-and-mobile-security-mexican-journalists-and-bloggers.

[59] SYRIA JUSTICE AND ACCOUNTABILITY CENTRE. Violations Database, 2014. http://syriaaccountability.org/database/.

[60] THE GUARDIAN PROJECT. Secure mobile apps. https://guardianproject.info/apps.

[61] TOR. Tor Browser Bundle. https://www.torproject.org/projects/torbrowser.html.en.

[62] TOW CENTER FOR DIGITAL JOURNALISM. Journalism After Snowden. Columbia Journalism School, 2014. http://towcenter.org/journalism-after-snowden/.

[63] UNGER, N., DECHAND, S., BONNEAU, J., FAHL, S., PERL, H., GOLDBERG, I., AND SMITH, M. SoK: Secure Messaging. In *Proceedings of the IEEE Symposium on Security and Privacy* (2015).

[64] WHISPER SYSTEMS. RedPhone and TextSecure. https://whispersystems.org/.

[65] WHITTEN, A., AND TYGAR, J. D. Why johnny can't encrypt: A usability evaluation of pgp 5.0. In *Proceedings of the 8th USENIX Security Symposium* (1999).

[66] ZETTER, K. Sony got hacked hard: What we know and don?t know so far. Wired, Dec. 2014. http://www.wired.com/2014/12/sony-hack-what-we-know/.

[67] ZIMMERMANN, P. R. *The Official PGP User's Guide*. MIT Press, Cambridge, MA, USA, 1995.