Susan E. McGregor*, Franziska Roesner, and Kelly Caine

Individual versus Organizational Computer Security and Privacy Concerns in Journalism

Abstract: A free and open press is a critical piece of the civil-society infrastructure that supports both established and emerging democracies. However, as the professional activities of reporting and publishing are increasingly conducted by digital means, computer security and privacy risks threaten free and independent journalism around the globe. Through interviews with 15 practicing journalists and 14 organizational stakeholders (supervising editors and technologists), we reveal the distinct—and sometimes conflicting—computer security concerns and priorities of different stakeholder groups within journalistic institutions, as well as unique issues in journalism compared to other types of organizations. As these concerns have not been deeply studied by those designing computer security practices or technologies that may benefit journalism, this research offers insight into some of the practical and cultural constraints that can limit the computer security and privacy practices of the journalism community as a whole. Based on these findings, we suggest paths for future research and development that can bridge these gaps through new tools and practices.

Keywords: Journalism, Usable Security, Usable Privacy, Organizational Practices

DOI 10.1515/popets-2016-0048
Received 2016-02-29; revised 2016-06-02; accepted 2016-06-02.

1 Introduction

A free and open press is a central characteristic of successful democracies and those societies moving toward democracy. Technologies can facilitate a free and open press by involving more people in the journalistic process (e.g., [1]) and reducing barriers to communication. However, technologies can also curtail these freedoms by creating computer security vulnerabilities—enabling, among other risks, leak prosecutions (e.g., [2, 3]) and cyberattacks targeted at news organizations (e.g., [4–6]). These security issues directly impact privacy and confidentiality goals for journalist-source communications. They contribute to "chilling effects" in which sources become reluctant to communicate with journalists about potentially sensitive issues [7], and they functionally abridge legal protections afforded to journalists in countries like the U.S. to protect the identities of sources [8]. In short, they limit the free operation of the press.

On the Need to Study Journalistic Organizations. Despite both the pressing need for—and increasing threats against—free and independent journalism around the world, the computer security and privacy community does not have sufficiently robust answers to scientific questions about how to design and implement usable and effective security- and privacy-enhancing tools for journalists and journalistic organizations. Though journalists are a community of interest to privacy and security scholars—in 2014 alone, multiple researchers (e.g., [9, 10]) argued that journalists are likely surveillance targets, and therefore a primary user group for proposed and/or evaluated digital security-related technologies—the scholarship on their actual needs and practices is quite limited within the computer security and privacy community.

Though recent work [11] examined the practices of *individual* journalists, this research left unanswered many questions about the role of journalistic *organizations* in the security and privacy choices of the journalists they employ. And while journalistic organizations share many features with other types organizations, our findings indicate that journalistic organizations have unique characteristics that affect their computer privacy and security risks and outcomes.

Our Study and Findings. To bridge this knowledge gap, our work considers the computer security and privacy practices, attitudes, needs, and challenges specifically for journalistic organizations as a whole.

Through interviews with 14 organizational stakeholders (supervising editors and technologists) and 15 practicing journalists at well-respected media organi-

***Corresponding Author: Susan E. McGregor:** Columbia Journalism School, E-mail: sem2196@columbia.edu
Franziska Roesner: University of Washington, E-mail: franzi@cs.washington.edu
Kelly Caine: Clemson University, E-mail: caine@clemson.edu

zations, we find that journalistic organizations and individual journalists share certain motivations towards computer security, particularly with respect to source protection and the reputational risks of a computer security breach. However, we find important differences in how these motivations translate to day-to-day security concerns and behaviors: for example, individual journalists rarely or never reported phishing, password strength, or the exposure of data to third-party cloud service providers as security concerns, though these were among the top concerns for organizational stakeholders.

We find that these differences lead to broader computer security challenges in the journalism community. For example, as organizational stakeholders struggle to balance various priorities in the face of limited resources, security and privacy concerns that have only a rare—if catastrophic—effect on their news "product" are pushed down the list. Individual journalists, meanwhile, must collect their "raw materials" from human sources and so are hesitant to introduce any barriers to those communications.

Critically, sources receive no direct goods, services, or compensation in return for the information they provide, and journalists are treated more as autonomous peers than subordinates in journalistic organizations. Both of these characteristics differ from norms in other fields where individuals share sensitive information with employees, such as retail, medicine or law. As a result, neither journalists nor their organizations have sufficient leverage to simply mandate that more secure tools or protocols be used by *either* journalists or their sources.

Our findings demonstrate that these structural and cultural features of journalistic practice have concrete implications for the design of secure, usable communication systems for this community. For example, the above issues make any single, centralized portal for all journalist-source communication impractical. Moreover, our findings reveal that journalists are unlikely to use a solution that they do not fully understand. We discuss further recommendations for computer security tools and practices within journalistic organizations, as well as opportunities for future work, in Section 6.

Contributions. Unlike prior work that studied the computer security and privacy attitudes, practices, and needs of individual journalists, we take a step back and consider the broader journalistic ecosystem. We make several contributions:

1. We identify key differences in the computer security priorities and concerns of individual journalists and organizational stakeholders (Section 4.1).
2. We surface broader challenges to robust computer security and privacy practices that arise within journalistic organizations (Section 4.2).
3. We highlight unique features of journalistic organizations, compared to other types of organizations, that have implications for security- and privacy-enhancing technologies intended for journalists (Section 5).
4. We provide lessons and recommendations from our findings, including paths for future research and development (Section 6).

2 Context, Related Work, and Motivation

We provide context and overview related work, identifying a need to study computer security and privacy specific to the journalistic context, with a comprehensive focus on both journalists and journalistic organizations.

2.1 Security Risks in Journalism

In recent years, the security of journalist-source communications has received increased attention, in part due to concerns about government surveillance [7, 12, 13] as well as legal attacks against sensitive sources [3, 13] in the U.S. and Britain. A number of high-profile technical attacks in recent years have also targeted journalistic and related organizations [4–6, 9, 10, 14].

These attacks have highlighted a need for secure communication and data management within journalistic organizations, and have helped spur the development of secure communication tools designed specifically for journalists (e.g., SecureDrop [15] and Dispatch [16]). The journalism community, meanwhile, has responded by developing digital security guides and trainings centered around existing technologies (e.g., [17, 18]).

Unfortunately, computer security practices within journalistic organizations suffer from both the usability limitations of existing computer security tools, and insufficient resources to robustly address or prioritize security issues. For example, over the last decade, many journalistic organizations have transitioned to third-party services like Gmail for their corporate email, and many new ones rely on such services from the start [19, 20]. These decisions have largely been driven by the need for lower costs and better usability [21]. Cost concerns and competitive pressures also drive news

organizations to rely increasingly on journalists' use of personal devices for work, especially mobile phones. As confirmed in our interviews, news organizations thus rely on a heterogeneous and generally unmanaged range of devices and communications systems, creating an environment of increased computer security risks.

2.2 Security, Usability, and Journalism

In addition to tools developed specifically for journalists mentioned above (e.g., [15, 16]), the technical computer security community has built many secure communications tools over the years, including OTR for encrypted chat [22], PGP for encrypted email [23], Tor for anonymous web browsing [24], and many others [25].

Yet these tools rarely see widespread adoption among either journalists (e.g., [26–28])—despite the significant risks they face—or the broader population (e.g., [29–31]). Moreover, scholarship on the actual computer security needs and practices of journalists and their organizations is limited. For example, no papers published at PETS in the last five years address the specific needs of journalists or journalistic organizations.

One recent study [11] focused on individual journalists, and revealed that limited usage of existing tools results not only from standard usability challenges but because these tools are difficult to integrate into the working processes of journalists (e.g., communicating with long-term sources). This work did not, however, evaluate journalists' practices in the context of their organizations. We bridge this gap by considering organizational stakeholders beyond individual journalists. We also surface unique aspects of journalistic culture that may influence the adoption or use of security- and privacy-enhancing tools in journalistic organizations.

From an HCI perspective, others have studied journalism more broadly than security. For example, Garbett et al. [1] studied the role of citizen journalism; Diakopoulos et al. [32] investigated methods for journalists to identify useful social media sources; and Taylor et al. [33] discuss the potential for citizen journalism to help communities take a role in a technological design process that takes into account their community's specific needs ("insight journalism"). These investigations highlight that the complexities of the journalistic process go beyond the level of individual journalists.

2.3 Usable Security for Individuals and Organizations

A large body of work exists on the interaction between individuals and organizations and its impact on security (e.g., [34]). While usability is a major issue in the adoption of secure technologies (e.g., [31]), organizational culture also plays an important role (e.g., [35]). Our work therefore seeks to provide a deeper understanding of both the task-specific usability issues that journalists face when using secure communication tools, and the ways that the unique culture of journalism and journalistic organizations affects the security approaches they employ. For example, in line with findings around other user groups (e.g., [36]), we find that journalists' level of understanding about secure communications plays a role in their use of certain tools. As we discuss in Section 5, we also identify important differences between journalistic institutions and other types of organizations that have implications for their computer security challenges, attitudes, and practices.

3 Methods

To study the computer security and privacy needs and practices among different stakeholders within journalistic organizations, we conducted semi-structured interviews with 29 participants: 14 organizational stakeholders (seven editors and seven technologists) and 15 individual journalists. All participants were current employees at media organizations, including print, online, broadcast and wire services, ranging in size from small, new, U.S.-focused media organizations to large, established, international media organizations.

We recruited participants through our existing professional network within the journalism community. Editors and technologists were recruited through person-to-person conversations with organizational leaders who then referred us to appropriate individuals. Individual journalists were identified through snowball sampling and were often recommended by a leader within the organization based on expertise and availability. While organizational leaders often first recommended we speak with their most security-conscious or -knowledgeable staffers, we explicitly requested also meeting participants who were non-experts, in order to ensure a broad representation of perspectives.

3.1 Participants

Because editors and information technologists both represent the organizational perspective, we refer to them collectively as organizational stakeholders. We selected these participants according to the following criteria:

– *Editors* are authorized to make editorial decisions for one or more journalists within the news organization who report directly to them. This means that the participant had the ability to approve pitches and stories for publication, as well as make scheduling and other resourcing decisions for coverage.
– *Technologists* are knowledgeable about and have influence on the organizations' information technology and, where applicable, computer security practices (e.g., one participant's title was "head of IT").

Individual journalists were selected according to the following criteria:

– *Journalists* are full-time employees of well-respected media organizations including print, digital and broadcast outlets as well as wire services, who regularly communicate with human sources in the process of reporting and publishing original journalism

Interviews with were conducted between November 2014 and September 2015. Interview length ranged from 15 minutes to one hour, and were conducted either in-person ($n = 23$) or via telephone/online video/voice conference ($n = 6$). The majority of participants were based in the U.S. and were interviewed in English, but eight participants were based in Europe and some of those interviews were conducted in the native language of the interviewee and translated during transcription. Seventeen participants were men (including all of the technologists) and twelve participants were women.

The participants in our study represent a broad range of privacy and security needs. Organizational stakeholders include those with editorial and/or technical responsibility for highly sensitive topics and materials—including those of potential interest to nation-states–as well as less sensitive, general interest coverage. Likewise, some journalist participants dealt regularly with highly sensitive topics and materials and had firsthand surveillance experience, while others described their work as non-sensitive and routine.

3.2 Ethical Considerations

Our entire protocol was IRB approved. Furthermore, we considered ethical principles such as beneficence, minimal risk, voluntary consent, and respect for privacy. Specifically, because of the potentially sensitive nature of some of our inquiries, we made explicit efforts not to leave a digital trail that could later identify the participants we interviewed. When organizing interviews, we avoided corresponding directly with interview subjects via email in advance of the interview. Instead, the interviewer typically corresponded with an organizational leader who then suggested potential interviewees. Those who met the criteria and were available participated.

During the interviews, we were careful not to elicit any protected information which journalists would normally not share, such as details about specific stories or sources. In accordance with concerns expressed to us during recruitment, we agreed not to publish organizations' specific security protocols so as not to compromise the effectiveness of those practices.

All participants agreed to being audio recorded during the interview and all participants answered all of the questions in the interview script. We stored and transmitted audio recordings and de-identified transcripts only in encrypted and/or password-protected form.

3.3 Interview Script

We varied our interview script by the type of participant: journalist, information technologist, or editor.

Organizational Stakeholders. Interview questions for editors and technologists were divided into three general sections: questions about strategies and policies, questions about tools and software, and questions about organizational culture and challenges.

For editors, the first section focused on what kind of trainings were provided to newsroom staff, whether the organization made specific recommendations to journalists about how to manage information related to stories, and how information security did or might factor into decision-making about publication decisions (e.g., when to publish a story). This section also assessed the editorial participant's awareness of information security resources or personnel within the organization.

For technologists, the first section addressed similar questions, but focused on whether information-security specific trainings and/or recommendations were made to journalists by the participant's department,

and whether information security for journalists was an explicit mandate for someone within the department.

The tools and software portion of the interview for both groups focused on security and privacy software that was available to or in use by journalists. Editors were asked about any software they or their team had attempted to use—with or without success—as well as unaddressed technology needs related to security. They were also polled about non-technological security challenges and what would be required to address them.

Technologists were queried more specifically about the tools, technologies, and computer administrative rights to which typical journalist users in their organization would have access. We specifically asked about whether any security or privacy software (specifically OTR and GPG) was part of users' default computer profiles, and whether individuals had administrator rights to install new software. We also asked about third-party and cloud-based services licensed by the company, as well as what digital storage and communication services the organization provided directly (e.g., a virtual private network, shared network drives, etc.).

The final portion of the interview addressed organizational culture and challenges. Participants were asked to assess the most serious information security issue faced by the organization, and to characterize the outcome should that issue arise (e.g., if the website was hacked). Editorial participants were then asked about challenges they had encountered or anticipated in implementing stronger security or source protection policies in the newsroom. Technologists were asked about both technical and non-technical challenges to implementing stronger information security, and were asked prioritize two journalist behaviors as the top of their "wish list" for improving information security in their organization.

Journalists. Interview questions for journalists focused on their communication with sources, computer security needs, and data management practices. These were elicited in two parts: the first asked participants to answer questions about source communications by calling to mind their actual interactions with a specific source from a recently published story. The second focused on general questions about data management and sharing, as well as the journalist's own computer and information security concerns and resources, including those in their personal network.

	Concern	Journalists	Organizations
Shared (Sec. 4.1.1)	Source Protection in Communication	6	8
	Reputational Risks	5	7
	Competitive Value of Risk of Infosec	3	4
Differing (Sec. 4.1.2)	Sources Drive Comm. Method	7	3
	Phishing	0	8
	Password Sharing	0	10
	Weak Passwords	1	4
	Third-Party or Cloud Apps	1	7
	Limited Resources	0	12
	Liability / Libel	0	4
	Protecting Journalists Abroad	1	3

Fig. 1. Table 1. Journalist ($n = 15$) versus Organizational ($n = 14$) Stakeholder Concerns Related to Computer Security.

3.4 Data Preparation and Analysis

Once all interviews were complete, we transcribed the audio recordings and coded the resulting transcripts using an iterative inductive process [37]. We then identified themes based on the coded transcripts.

4 Results

We organize our results around two overarching themes: (1) specific shared and differing security concerns between organizational stakeholders and individual journalists, and (2) broader challenges to organizational computer security in journalism. Together, these results reveal opportunities for improving the collective security practices of journalists and journalistic organizations.

4.1 Journalist versus Organizational Computer Security Concerns

Overall, we found that while individual journalists and organizational stakeholders share similar security motivations (e.g., protecting source identities), the way each group prioritizes computer security and privacy threats and concerns can differ drastically in practice. Table 1 summarizes these results, and this section discusses these findings in detail.

4.1.1 Shared Priorities

We begin by highlighting two areas of shared priority that drive computer security choices for both journalists and organizational stakeholders: the need to protect source identities and the reputation of the organization.

Source Protection. Both individual journalists and organizational stakeholders described the protection of sources as a critical information security concern. For example, one journalist said:

> My sources trust me to keep their information. It would be a problem for my news organization, to not be able to protect my sources, to protect the files or documents. (J5)

Organizational stakeholders expressed their concerns about source protection in particularly urgent terms. For example, while one journalist acknowledged that exposure of a source's information "would probably not be great" (J11), organizational stakeholders tended to describe source protection as "vital", "crucial," and "critical." As one editor put it:

> [Source protection is] terribly important. It's important in the U.S. because there are laws about that, but it is particularly important overseas where governments can intimidate those who talk to Western reporters and/or take reprisals against our local staff in those countries. (E5)

Organizational stakeholders also expressed a sense of responsibility for the security practices of journalists affiliated with their organization. For example:

> If [a journalist is] texting from a personal account and I didn't know about that or didn't strive to prevent that and then that somehow gets into the hands of the public when we promised anonymity—and causes whatever results the person was trying to prevent by asking for anonymity and we agreed were reasonable by granting it—that's a grievous journalistic error. (E3)

While these findings suggest that it is the responsibility of both individual journalists *and* the journalistic organization to protect sources, only one organization in our sample included secure communication tools by default, as we discuss in Section 4.2.1.

Reputation Protection. Like source protection, reputational concerns were also prevalent in both groups of participants (five of 15 individuals and seven of 14 organizational stakeholders). For journalists, however, reputational concerns primarily revolved around the worry that the failure to protect a source would affect the ability to attract future sources.

Organizations' concerns about reduced access to sources, however, was overshadowed by the possibility that failure to protect a source would compromise the credibility and integrity of the brand; both the importance and fragility of the organization's reputation was mentioned by multiple stakeholders:

> [We] have, I think, a pretty good reputation. But it could get blown away in an instant, so we have to make sure that we protect everyone, because if that gets out, then we'll never live it down. (E2)

> [One of the] really serious problems is the brand image, the damage to the brand. If you're not deemed trustworthy. . . . Trust and reliability are indispensable to us. (E1)

So, while both individual journalists and organizational stakeholders are concerned about protecting sources, their motivations for doing so diverge: individual journalists worry about *their own* ability to attract future sources, while organizational stakeholders worry about brand image, and the ability of *all* their journalists to attract future sources. Nevertheless, both individual journalists and organizational stakeholders are strongly and similarly motivated to protect sources. This motivation may lead to journalistic users being willing to adopt new technologies, spend more time using technologies, and otherwise sacrifice some amount of ease of use and convenience [38]. As we discuss in Section 5, however, even motivation cannot compensate for missing functionality.

4.1.2 Differing Concerns

Though both individual journalists and organizational stakeholders identified source protection and reputation management as substantial motivators of better computer security practices, the way priorities manifest in practice can differ dramatically. For example, several of the most pressing concerns for organizational stakeholders—such as libel, phishing, and manageable computer security practices—were not mentioned by even a single individual journalist.

Sources Drive Communication Method. Since one goal of individual journalists is to gather information from sources, their concerns include their *sources'* technical abilities and access to technology. Echoing previous work [11], we find that lowering the barrier to communication is critical. As one journalist put it:

> In my experience, taking down barriers is the most important thing to source communication for 99% of the people you need to access as a journalist. (J14)

As a result, the communication methods used by journalists are driven largely by the preferences of sources; even journalists who understand the risks of insecure communication methods may choose those tools over secure ones, if that is what the source prefers. In general, journalists expressed deference to time, availability, and convenience of sources over security. When asked if they would feel comfortable asking a source to use a specific form of communication, journalists agreed:

> Absolutely not. I would never impose any kind of burden on a source to communicate in a way that they're not used to. You're taking their time. (J14)

> There are few sources that I've had that I would feel comfortable asking them to use, like, hyper-specific technologies to talk to me through, like a different app, or a funky encryption service, or something. (J13)

While some of these concerns were acknowledged by organizational stakeholders, they generally expressed less concern about the repercussions of losing a particular source. For example:

> I mean, my fear for the secure communication with sources is definitely like, I don't want [a source] to not want to wait for someone [e.g., a reporter] to figure something out and so they go somewhere else. But that's not, like, an existential fear, because if we lose a story, then I have plenty of ways to communicate with a new one. (E2)

While organizational stakeholders' focus is on the security and practices of the organization's employees as a whole, perhaps because they worry primarily about organizational reputation, individual journalists "on the ground," are more focused on ensuring a source is comfortable and willing to talk. Whereas an organizational stakeholder may be willing to lose a source in a case where they would not use secure communication, individual journalists may not be.

Phishing. Unlike source protection and reputational concerns, computer security issues not directly connected to newsgathering—such as phishing and password practices—were articulated only by organizational stakeholders. Eight of 14 organizational stakeholders expressed concern about phishing attacks—a concern that was shared equally between editors and technologists. By comparison, none of the 15 journalists interviewed mentioned phishing as a computer security concern.

Concern about phishing among organizational stakeholders stemmed from two distinct characteristics of this type of attack: the pervasiveness of the tactic and the potential severity of its consequences. Asked to characterize the organization's biggest security risk, one technologist said simply:

> Phishing, and DDOS. Because they're cheap and they're effective. (T2)

In terms of potential severity of the consequences, several recent academic studies discussed targeted phishing as a primary cause of compromise for politically-involved organizations (such as NGOs, activist organizations, and journalistic organizations) [9, 10]. Compromising the account of one of an organization's employees may provide access to significant sensitive information, including source identities and unpublished stories. For example, one technologist commented:

> We had a targeted phishing attack against us, that, after doing some analysis, we determined it was probably SEA [the Syrian Electronic Army]. . . . We had a couple of people whose email accounts were compromised. (T3)

In other organizations, the consequences have been much more severe (e.g., [39]).

One editor interviewed also highlighted an incident where a phishing attack resulted in significant downtime within the organization, a serious business and credibility issue for journalistic outlets where, unlike banks, for example, 24-7 operations are viewed as a requirement:

> The company was attacked by an international group. . . . Suddenly at 10pm everyone is getting a phone call [from IT] saying you've got to change your password now. We've had other phishing things but this one took the whole server system down, the whole nine yards. (E5)

The always-on business cycle of journalism also means that recovering from a phishing attack may be particularly challenging, as the timeliness and currency of information are of significant competitive value. Interrupting the publication flow and/or reverting to backup data even a few hours old can be commercially damaging.

The disparity between the individual and organizational perspectives here is notable. While many organizational stakeholders expressed concern about phishing, no individual journalists mentioned this risk. It is not clear why journalists seem unconcerned, or at least less concerned, about phishing. One possibility is that journalists are aware of the risk, but may not consider it their responsibility. As one technologist put it:

> Some people have the attitude, I don't wanna be bothered by this stuff, can't IT just fix it, don't you have something that can keep everything secure, that doesn't require me to do anything different at all. (T1)

Another possibility is that journalists are simply unaware of the risk. If so, then why are journalists unaware when the organization is keenly aware? Do journalistic organizations offer training that includes information about phishing, and if so, why it is ineffective? One possible answer may be suggested by the resource limitations we discuss in Section 4.2 below: that the attention paid to computer security by all parties must be balanced with other competing concerns.

Password Security. Password security was also mentioned by all technologists interviewed and three of seven editors as a top computer security concern, both in terms of password sharing/reuse and password strength. Several organizational technologists put improving password security and practices at the top of their "wish list." As one described it:

> One of [the items on my wish list] would be to improve password security. . . . I think that there's probably a lot of people who aren't actually using password databases and who are probably reusing passwords sometimes, and who are using weaker passwords than they need to and things like that. (T6)

This desire also extended to personal accounts and devices, congruent with the fact that all organizations where interviews were conducted had "bring your own device" practices. As another technologist mentioned:

> I guess the first would be just better personal password policies. (T3)

By contrast, only one individual journalist mentioned password sharing, but as a positive means of information management (to collaborate with colleagues), rather than a security risk. Again, the disparity here is worth considering. Why do organizational stakeholders—but not individual journalists—consider password security to be such a high priority? Perhaps editors and technologists are (as a result of their positions in the organization) more aware of incidents involving password security, and/or are trained to be attuned to this risk. If either of these is the case, why is this information not making its way to end users (journalists)?

Third-Party and Cloud Applications. Finally, while seven of 14 organizational stakeholders expressed concerns about the computer security risks of using third-party and cloud applications, these issues did not appear to occupy the attention of individual journalists.

For example, prior work [11] indicated that individual journalists did not report computer security concerns associated with third-party applications or the remote syncing of data. Yet technologists we interviewed expressed concerns about both USB drives and third-party services, a concern shared by savvy editors as well. As one said:

> Sometimes I'm just walking through the organization and I'll see someone with an Evernote open—and it's like, just making sure that you're not putting your source phone numbers in there! If you want to keep your recipes in there that's fine, but be careful. (E1)

Likewise, while technologists saw benefits in cloud infrastructure, they also appreciated its risks:

> We wanna take advantage of all the good benefits you get from being in the cloud. Scalability, higher performance, bigger global footprint, etc. But as we've learned, these parties can get subpoenaed and they can be gagged, and so we definitely first and foremost think about what is the data that we think about possibly migrating to the cloud, and from an infosec perspective is it even a candidate? (T1)

At some smaller organizations—where budgets were not always sufficient to support an in-house information technology department—concerns about third-party services also extended to physical computer and networking infrastructure, which was sometimes maintained by third parties, rather than direct employees.

While better-resourced organizations in industries like retail and law may have purpose-built (if less than usable) systems that satisfy unique needs, for both budgetary and efficiency reasons, journalistic organizations increasingly use "off-the-shelf" software for communication and coordination. One side effect of this is that secure communications tools compare particularly unfavorably with these large-scale solutions. For example, one participant described the challenge of encouraging the use of secure tools on a distributed project:

> I had to call the editor running the story to say, let's just make sure we're being careful here, because Google will turn this stuff over to the feds in a heartbeat. . . . The problem with Google Docs is it's awesome – I mean it's so seamless and intuitive. Much more so than some of the more secure solutions. (E1)

4.2 Challenges to Organizational Computer Security in Journalism

Stepping back, our interviews with organizational stakeholders also surfaced several broader themes directly related to the systemic challenges to organizational computer security in journalistic organizations, in part due to the disparities in day-to-day concerns and priorities among different members of the organization. While many of these challenges echo issues present in other types of organizations, we discuss further in Section 5, there exist important ways in which these issues are particularly challenging in the journalistic context.

4.2.1 Supporting Software

An organization's technical staff is tasked with supporting a variety of hardware and software for the employees of that organization. This task is simplified when the necessary tools are standardized across organizational users, when those tools come with sufficient external support and/or can be sufficiently controlled by the IT department. As a result, for example, un- or semi-supported projects like GPG, or externally-managed cloud services like Google Docs can be more challenging to adopt than explicit enterprise solutions like Microsoft Outlook. For example, one technologist interviewed discussed Google Docs:

> It's a case of: Who owns this? Who's going to pay for it? Who's going to pay for the licenses? And then it becomes an issue around: is this a strategic imperative? Who controls it? (T5)

As a result of the difficulty of supporting one-off tools, technical staff members may be hesitant to support specific computer security tools used by only a small number of individual journalists. For example, one technologist mentioned learning about new security tools from journalists themselves, but admits some reluctance about supporting such tools:

> If you come to me and tell me that you need to be able to encrypt the email that you're writing to a source, we're at the point now where we're going to tell you that the tool that you are going use is GPG 4.0. We're not going to go use some other tool. We find some tool and standardize on it, until we find some reason that it's no longer going to serve our standard. (T1)

The challenges of supporting software also extended to what users were provided with by default; only one organization in our study provided computer security software by default on regular user profiles. Moreover, only 6 of 15 journalists had the admin privileges required to install additional software. For technologists, this was in part a support issue:

> Historically, [users] had too many administrative rights on the PCs and it got them into trouble. They would just install something that would conflict with something else on their machine. (T1)

One potential side effect of this approach is that newer tools—which necessarily have lower adoption rates—may never be practically available to institutional journalists even if they are more usable or more secure than more established alternatives.

4.2.2 Distributed and Collaborative Culture

The inherently distributed and collaborative nature of journalism presents specific challenges to communicating securely. As one journalist put it:

> We try to use the most secure tools possible. And I think the problem was that at first we were only two or three . . . and now we are maybe a dozen. And as most of my colleagues are not really good with technology we have to lower our expectations in security. (J9)

Another participant expressed a similar difficulty: the most trusted secure chat solution (OTR) doesn't support multi-party chat.

> I use CryptoCat for stuff that is for someone that I know I'm not going to be able to figure out how to get OTR on—it's so much simpler. . . . It's also nice because it has a group function, and I haven't really found. . . I don't know how secure it is, so I wouldn't necessarily use it for the most sensitive of things, but for something that is sensitive and I need to have a group conversation about, I would go for that because it's simple. (E2)

This finding has implications for the design of secure systems for journalistic practice: targeted solutions should consider all stakeholders and communication partners, not just individual journalists and their sources. The ability to communicate securely with colleagues is a critical part of the journalistic process.

4.2.3 "Us-vs.-them" Mentalities

Though the pressure to adopt certain computer security tools may come from individual journalists, as noted above, organizational stakeholders must typically manage the computer security of an entire media organization. As a result, an "us-vs.-them" mentality can sometimes begin to characterize the attitudes of organizational stakeholders towards individual journalists, or of editorial staff towards IT department staff. For example, one editor described enforcing better computer security practices among journalists as a problem of "herding cats" (E4) while another expressed frustration with his organization's IT department:

> It's the journalists dragging the IT people kicking and screaming and saying, you need to think about China, you need to think about Russia, because we have people there. They think of it very much in hardware terms. (E5)

We also found evidence that the culture of journalism—despite the presence of official hierarchies—functions in a largely egalitarian, peer-oriented way. When speaking about security, it was clear that institutional actors were uncomfortable with simply imposing requirements:

> Occasionally reporters will ask or start using services that we're a little less comfortable with that are maybe a little more convenient . . . and there's no prohibition but we sit down with them and say, "We need for you to understand the risks associated with this." (E1)

There was also the sense that imposing requirements would be ineffective:

> [Security] has to be enforced in some way. Not necessarily with punitive repercussions, but something that doesn't allow people to work around it. Journalists, what they are good at, is overcoming an obstacle that they don't choose to deal with. (E5)

4.2.4 Limited Resources: Secure Journalism Comes with a Cost

Maintaining strong information security and data management practices at a journalistic organization requires devoting significant resources exclusively to this purpose. These resources must be gleaned from an existing pool of limited people, money, skills, and attention otherwise focused on journalistic and business tasks.

Uncertain priorities. Devoting resources, in terms of people or infrastructure, to computer security costs money—money that may otherwise be put to other uses within the organization. While downtime in the organization cost credibility, it was often unclear what "uptime" was worth. In the words of one technologist:

> I sort of ran the numbers. . . . That would cost us anywhere from $25-50K, just in infrastructure costs alone, right? And like, we can scale up. The way that we've architected our environment, we can scale up to—whatever we need. But, it costs money. . . . I can't make those decisions, about whether or not we take down content because it costs us 100 grand over a two-day period, right? That's something that [the editorial leaders] will have to decide. So, I want their input on that kind of stuff. I mean, if we're coming out with a new application tomorrow, we could spend a lot of money securing it. We can make it a hardened target. But do we need to do that? (T2)

Limited Time. One of the most compelling and frequently cited issues our interviews revealed was the broader opportunity cost of computer security. This was particularly true for editors and technologists, who often referred to managing competing priorities when asked about the role of newsroom source protection and information security. As one participant put it:

> There are lots of other fires to put out every day, so I think it's probably an issue that doesn't get the priority in our newsroom that it deserves. (E3)

The cost of computer security was also felt as a limitation on executing journalism itself. As one editor said:

> There's a kind of like an encryption tax on the work of journalists these days. . . . We have to spend time doing things that we otherwise wouldn't do in order to communicate securely with sources and with each other and to responsibly use documents that we have. And it takes time. It means that we have less time to talk to people, to go and travel, etc. We still do all those things, but there's a chunk of our time that's spent on security, and not on other forms of reporting. (E6)

Limited Attention. Even when computer security interventions were taken, however, editors and technologists alike expressed the need to carefully manage the limited attention they felt journalists had for these issues. As one technologist said:

> We always feel like we're vying for part of a limited attention span. If you want to communicate something, you want to be sure you have their attention. . . . If you throw too much at them, none of it gets attention. . . . If you tell somebody come to this workshop, we're going to tell you how to not get phished, or how to keep your phone call encrypted—

> unless you have cookies, two people are going to show up. (T1)

Limited Expertise. Another frequently cited limitation on better computer security was insufficient expertise within the organization. At times, this limitation prohibited the adoption of very specific tools or protocols, as one technologist noted:

> I would love to force people to use a password manager, but that's not realistic at this point—frankly because I'd probably be the one who'd end up doing desktop support on that and I don't have the time for that. (T3)

Indeed, prior work [11] found that individual journalists often did not feel that they had someone with technical expertise within their organization to whom they could go for help with computer security related issues.

In other cases, insufficient staff expertise simply creates an imbalance of work:

> It ends up being that that one person has way too much work to do to support everyone in the office. And then there's only so much that you can do remotely to support people. (T6)

Limited Understanding. Expert staff in the strictest sense, however, was not the only way in which expertise limitations were felt. Multiple participants indicated the importance of their own need to understand how computer security tools work:

> Having people that are journalists and actually want to know everything, they're like: "Wait, I don't understand. I need to understand how this functions before I start to use it." Which is also a thing of "I need to understand how it functions so I feel comfortable using it." And so it's not that hard in abstract to think like, "Great, you're basically putting everything into a cipher and then you're sending that cipher to someone else and you have two different keys." Like, it's not that crazy, but when you start to actually execute it you're like, "Wait, I have to have this key, and if this key gets out then I'm in trouble, but this is also called a key but this is something I share with everyone?" (E2)

In other words, individually understanding the how and why behind computer security practices and tools was an important factor in being willing to use them. This attitude highlights an opportunity to engage with individuals on these issues and change their behaviors:

> My initial response to being prompted to set up two factor authentication on my personal accounts—like on my Gmail account or my Facebook or wherever—was deep skepticism, because it just felt like another corporation asking for my phone number. . . . It was only really after . . . the whole tech team gave kind of a broader and clearer explanation of why it matters, and it didn't just seem like some kind of fishy thing from a faceless corporation, but more like, you know—here's a person I trust who's looking out for my company telling me why this matters for us as a company. And shortly after we went to two factor for the company, you know, I sort of acquiesced to all of the various two-factor requests in the rest of my life as well. (E3)

As we discuss in Section 6, clear communication by organizational stakeholders with journalists about computer security goals and consequences is thus important. This observation also holds implications for the designs of computer security tools for journalists, which may see more adoption if their benefits are clearly explained.

4.3 Summary of Findings

Our findings suggest that individual journalists and organization stakeholders within journalistic institutions consider and prioritize different computer security and privacy concerns. Though both groups take very seriously their professional duties to protect sources and manage the organization's reputation, organizational stakeholders are focused more inward, concerned with the computer security practices of their employees (e.g., resilience to phishing attacks) and the tradeoffs in how to allocate resources. Individual journalists are tasked with collecting information from sources, and so their use of secure communication technologies is often influenced by the abilities and attitudes of sources; their concerns surrounding computer security lie more in whether and how to protect those communications, and less on their own individual behavior within the organization (e.g., password practices). As a result of these differing viewpoints and priorities, different organizational stakeholders in our interviews sometimes expressed frustration with other groups' failures to properly understand or support their priorities. Our interviews also surface additional important challenges to journalistic organizational computer security, including the challenges of supporting a variety of software across the organization and the need to balance computer security practices with other priorities in the face of limited resources (time, money, and expertise). These challenges expand on those previously identified in the context of individual journalists, such as the importance of a source's comfort level with computer security technologies [11].

5 Discussion: Journalistic versus Other Organizations

Naturally, some of the computer security challenges experienced by journalists and their organizations are also faced by other users and organizations. There are, however, many ways in which the resources, needs and culture of journalism differ significantly from other communities of practice, suggesting the need for additional research, tool, and strategy development to be focused specifically on journalists and their organizations.

5.1 Similarities to Other Organizations

At face value, many of the concerns expressed by journalistic organizations are similar to concerns of other organizations. For example, like many organizations, journalistic organizations must balance security concerns with other priorities in the face of limited resources of time, attention, expertise and money.

Phishing is also a common concern: phishing as a form of cyberattack is increasingly common, growing over 90% in 2014 [40]. Proposed solutions for phishing, such as training email recipients, have been unsuccessful [41]. Successful anti-phishing strategies that address either organizational practices in general and/or recipient practices can improve all organizations' information security, including journalistic organizations.

Similarly, insecure password practices are a pervasive problem across different organization types [35]. For example, people across organizational domains reuse passwords [42], indicating that journalists and journalistic organizations are not alone in their concerns about and less than optimal practices around passwords. In the case of journalists, there may be opportunities to use journalists' dedication to the protection of their sources as motivation to change their behaviors.

5.2 Unique Features of Journalistic Organizations

Beyond these basic similarities, our findings highlight several important cultural and functional *differences* between journalistic institutions and other types of organizations with comparable security needs. Thus, while on the surface it may seem that journalistic organizations could simply implement the types of organizational security practices in place at medical, legal, or retail organizations, solutions must consider the nature of journalistic organizations specifically.

5.2.1 Journalists as Atypical "Users"

As prior work indicates [11], journalists often select communication tools based on the preferences of their sources. In this sense, individual journalists may share some computer security needs and habits with other types of of "consumer-facing" industries, like retail and medicine. At the same time, however, individual journalists have both greater autonomy and responsibility in their work with sources. For example, while a retail clerk at a major chain store cannot independently choose to accept barter as a form of payment, individual journalists can (and do) accept as many forms of communication "currency" as possible. From an organizational standpoint, then, journalists are more like independent contractors than direct employees: they are responsible for delivering a content "product" to their organization, but they are individually responsible for how it is produced. As a result, journalists prioritize communicating with sources over security concerns, as this is the core "business" of journalism. As one editor put it:

> The effective [security] tools that are out there are pretty kludgey. And then because they're kludgey they get in the way of people being able to do their jobs. And I think given the choice of being information aware and secure and getting your story done, most journalists are gonna get their story done. It's about that simple. (E4)

Though an apparently simple solution would appear to be centralizing and mandating particular protocols or software, our research suggests that this approach would be a poor fit for the distributed and heterogeneous nature of journalistic organizations, as we discuss below.

5.2.2 Sources as Atypical "Clients"

Journalistic organizations are relatively unique in their desire to protect the privacy of an entire class of . . . organizational participant: sources. These participants are unpaid and unaffiliated with the organization itself, but are still a critical component of the journalistic product. While the cost and stress around legal concerns are substantial, the primary driver for journalistic organizations' desire to protect the security and privacy of sources is reputational, and ultimately existential: if

the organization does not protect the privacy of their sources, other sources will not work with them.

This observation supports existing research on privacy-enhancing behaviors suggesting that people avoid technologies or organizations that do not meet their privacy needs [43]. If journalistic organizations do not support sources in both revealing information *and* remaining private and/or anonymous, sources will be more reluctant to share information. Thus, the implementation and perception of more secure communications practices by journalists may also reduce source "chilling effects" that inhibit newsgathering [7]. Unlike organizations where "clients" directly benefit from their interactions with that organization (e.g., law firms), these issues are particularly existential for journalism.

5.2.3 Peer-Oriented Culture

One important feature of journalistic culture that we noted throughout our interviews was the dominance of peer-oriented attitudes despite formally hierarchical organizational structures. In journalistic organizations, for example, editors wield significant influence over individual journalists' work, including the ability to approve (and "kill") stories, and allocate time and financial resources for projects. That said, as discussed in Section 4.2.3, we noted a consistent reluctance on the part of editors we interviewed to mandate particular security practices for journalists in their organizations—or skepticism that such mandates would be effective.

5.2.4 Decentralized Control: De facto and by Design

Congruent with the reluctance on the part of organizational stakeholders to mandate particular systems or punish non-compliant journalist, our findings also reveal significant decentralization—both de facto and by design—in journalistic organizations' information security practices. This decentralization again differs from other, more top-down organizations where computer security practices can be more easily mandated.

De Facto Decentralization. Much of the decentralization of journalistic systems was attributable to the interaction between the wide range of populations and jurisdictions that media organizations touched, as well as to their limited resources.

> Our IT department is very reluctant to have a "one size fits all" approach. As a result they have no size that fits anyone. There is no good intersection between IT and the core of the business, which is news gathering. . . . It's like, here's an iPhone, good luck. (E5)

Decentralization by Design. Interestingly, however, there were instances in which the decentralization of information was treated as a security measure in itself, in a form of "security through obscurity."

> There's a case that we're working on about a sensitive topic, and I don't know the person's name . . . And I'm sure I could ask for the person's name, but there's no reason to know the person's name. . . . What you don't know you can't leak, you can't get in trouble with it, you can't get in trouble for having it. (E7)

A similar sentiment was expressed by one technologist:

> From a user support perspective, it would be good to store . . . passphrases, but our legal folks don't want to do that, because then *we* can be compelled to turn over passphrases by subpoena. Better that we not know them. (T1)

In this case, the very decentralization of information was perceived to help minimize its potential exposure points. This sentiment was echoed by another organizational leader, who commented:

> I feel like it's something that, even if [messaging service] is not—even if it was theoretically not super secure, it would be so hard to figure out what we were doing and where that is. . . . You're like, using something that's not the most popular is maybe the way to go. (E2)

Thus, the decentralization within journalistic organizations may have (possibly unintentional) security benefits, but it also limits the effectiveness of top-down mandates of computer security practices that may be effective in other types of organizations.

6 Lessons and Recommendations

Existing research on individual journalists' information security practices [11] recommends further work around issues of first contact, authentication, metadata protection and knowledge management. While valuable, these recommendations do not take into account the role of journalists' organizations in shaping their information security abilities and choices.

Additionally, though at first the security challenges of journalistic institutions resemble those of organiza-

tions in other industries, we identified functional and cultural aspects of journalistic organizations that set their needs apart. As a consequence, security solutions relying on conventionally opaque, tightly-coupled systems are unlikely to be useful in journalistic settings.

We therefore recommend that protocols and technologies designed for organizational journalists leverage well-known protocols, support multi-party collaboration, and clearly indicate the security processes and protections at work in a given tool. We close with reflections on opportunities for future work.

6.1 Rally Around Known Protocols/Tools

Recall from Section 4.2.1 that supporting a diverse range of software is a particular challenge for organizational participants. As a consequence, interoperability and adherence to known standards is viewed as critical:

> Probably the best tool, by far, is OTR, because everyone has a Gmail account, everyone has some sort of chat account, and since it's so seamless with Adium, and it's like once you have that open it's so simple, and it's great. (E2)

> ... We're gonna tell you that the tool that you *are* gonna use is GPG 4.0. We're not gonna go use some other tool. We find some tool and standardize on it. (T1)

Thus, we recommend that members of the technical computer security community wishing to develop tools for journalists work closely with organizational stakeholders to understand organizational needs and constraints, and to help support the deployment and maintenance of these tools. Without such support, the limited resources of journalistic organizations will greatly limit the adoption potential of new, and particularly of experimental, tools.

6.2 Support Multi-Party Collaboration

As we noted in Section 4.2.2, the production of journalism is inherently distributed and collaborative; privacy- and security-enhancing tools designed for the journalism community must support these functions. Our interviews suggest that efficiency and seamlessness of collaboration were high priorities for organizational stakeholders, and several journalists described using third-party services (like Google Docs) specifically to share information with others or between devices (e.g., with a home computer). In fact, our findings suggest that support for collaborative functionality is important enough that even security-conscious users will choose less secure tools that support these activities. Thus, while journalists are highly motivated to use security- and privacy-enhancing technologies, our broader findings suggest that these motivations will not overcome missing functionality. We therefore recommend that computer security tools seeking wide adoption consider implementations that support collaboration.

6.3 Clearly Communicate Security Goals and Consequences

Organizational concerns are often not visible or tangible to individual journalists, while these concerns are highly visible to organizational stakeholders. For example, organizational security concerns like password sharing and phishing rarely produce immediate or highly visible consequences at the individual level. This leads to an informational asymmetry between journalists and organizational stakeholders, who are often responsible for managing the consequences and identifying the security breach. As one technologist put it:

> If a user falls for a phishing attack, and they don't report it, and they don't even realize what happened—then, you know, what can you do at that point? It's only a problem when it becomes troublesome when it actually manifests into a security incident. And by that time it's too late. (T2)

Thus, helping journalists appreciate the impact of their individual behaviors on the organization may be a useful strategy for increasing secure computing behaviors. In one recent study, researchers demonstrated that employee attitudes toward organizational password policies affect password behaviors [35]. Similarly, we propose that properly explaining and contextualizing computer security practices for all journalists in an organization may help shift attitudes, priorities, and practices.

Better communication among the different stakeholders within organizations may also help overcome some of the gaps we observed. In the words of one technologist:

> My second biggest wish actually would be more communication and less whining. When something goes wrong, that they communicate it immediately, and not try to find a workaround. ... We don't have all the answers here. (T5)

In the other direction, clear communication from technologists is equally important:

> Having a technology team that can speak in fluid, persuasive non-jargon-ridden sentences is just like, an insane asset to any company. Because there's many ways to roll out security tweaks, and doing them where you make a clear and lucid case for what you're doing and why—there was just no pushback whatsoever. Everyone was just like, "OK, great. We'll do that." (E3)

When asked what pushback could be anticipated to efforts to impose further security in the newsroom, another editor commented:

> I think if explained, not really any. ...I think if it were presented as, this protects your sources—we are in the information business, we know that this is a contemporary issue in society, and in the industry. I don't think you're going to get any resistance from the journalists. (E5)

Thus, we recommend that journalistic organizations focus on clear communication channels among all stakeholders surrounding computer security issues. Building on the observation in Section 4.2.4 that journalists do change their security-related behaviors when they understand the issues, we also recommend that tool designers consider these issues within tools themselves—for example, providing clear user interfaces and explanations for the risks addressed and the benefits provided by security- or privacy-enhancing features.

6.4 Opportunities for Future Work

While our work clearly demonstrates that there are differences in computer security concerns between journalists and organizational stakeholders, as well as unique features of journalistic organizations compared to other types of organizations, a number of questions remain, presenting opportunities for future work.

Designing Tools and Practices. Our findings raised questions for the design of general organizational practices and specific computer security tools that can mitigate the challenges we observed. For example, organizational stakeholders devote significant effort to computer security issues not specifically related to journalism, like phishing and password practices. How can practices or tools better mitigate these issues so that organizational stakeholders may devote their computer security resources elsewhere?

Awareness and Education. We observed that journalists are willing to use computer security tools when they understand the risks they address and how they work. This finding suggests that education and awareness efforts can be successful in this space, particularly if they situate security in terms of other priorities and experiences. For example, training could focus on helping journalists understand that their computer security behaviors impact the safety of their colleagues and the reputation of the organization. Building on successful prior work in the area of anti-phishing education e.g., [44]) and lessons learned from industry (e.g. [45]), we believe that educating users about the security and privacy risks—and meaningful ways to mitigate them—has potential for significant impact in this space.

Considering all Stakeholders. Even when appropriate practices or tools exist, their adoption may fail in several ways: because sources are unable to use them and thus journalists avoid them; because organizational stakeholders are unwilling or unable to support them at the organizational level; or because information security priorities from organizational stakeholders don't reach or resonate with individual journalists. An important lesson from our findings for those developing computer security technologies for journalists is thus that it is not sufficient to make those solutions easy to use, or even to design them specifically for the journalistic process. Those seeking to develop computer security tools for journalists should include all organizational stakeholders in their design process. We must also understand the motivations and practices of sources, another set of primary stakeholders in the journalistic process, who have thus far not been studied in this context.

Other Journalistic Organizations. By interviewing people at major journalistic organizations that have staff members we could classify as technologists, our interviews could not provide a view of other organizations without even those resources. How can stronger computer security practices be best supported in such organizations? Our sample also included only participants from the U.S. and Europe (though many organizations had reporters working abroad). Western societies often afford journalism leeway that may not be granted in other locations. Therefore, our results may differ if we replicated this study with journalists who live in countries with weaker press and speech protections. However, because of Internet technology and the globalization of the media (e.g., [46]) we expect that some of our findings would translate.

Beyond Journalism. Finally, the journalism community has an existing framework and vocabulary for protecting the privacy of its members. This framework may be useful in other organizational settings, and it is possible

that other communities that maintain privileged relationships with a diverse range of constituents will benefit from further research on journalistic organizations. Lawyers, for example, arguably share many of the same responsibilities and concerns and challenges:

> The lack of universal use of [security technology] and the scariness of it for all kinds of reasons is problematic for journalists as well as others. And it just goes across the board. I mean it's like even emailing with lawyers, you know, who should know better. You know, they just have these little things that say, "This is confidential" and like, are you kidding? I had one experience with a prominent lawyer and he said, "Yeah, I've heard about this PGP stuff, I'd like to use it," but he was working for a big firm and his IT department basically said, "No, we just don't support that." (E6)

Thus, future work should investigate whether and how our findings apply in other domains.

7 Conclusion

A free and open press is a central characteristic of successful democracies and those societies moving toward democracy. Technologies can facilitate a free and open press, or restrain it. We argue that it is critical for the computer security and privacy community to systematically study security and privacy practices, attitudes, needs, and challenges in the journalistic context. We take a substantial step in this paper, focusing holistically on journalistic organizations. Our findings reveal important differences between individual journalists and organizational stakeholders (supervising editors and technologists), as well as broader organizational challenges to computer security and privacy. These challenges—many complicated by unique features of journalistic organizations compared to other types of organizations—have implications for the designs of security- and privacy-enhancing technologies and practices that will succeed in the journalistic context. We see supporting the computer security practices and needs of these organizations as critical to preserving a free press and all the societal benefits that come with it.

Acknowledgements

We thank our shepherd, Lorrie Faith Cranor, as well as our anonymous reviewers, for valuable feedback on an earlier version of this paper. We are also extremely grateful to our interview subjects for their participation. This work is supported in part by the National Science Foundation under Awards CNS-1513575, CNS-1513875, and CNS-1513663.

References

[1] A. T. Garbett, R. Comber, P. Egglestone, M. Glancy, and P. Olivier, "Finding real people: trust and diversity in the interface between professional and citizen journalists," in *32nd Annual ACM Conference on Human Factors in Computing Systems*. ACM, 2014, pp. 3015–3024.

[2] U.S. Supreme Court, "Risen v. United States," *SCOTUSblog*, Retrieved: June 5, 2014.

[3] A. E. Marimow, "Justice Department's scrutiny of Fox News reporter James Rosen in leak case draws fire," *The Washington Post*, May 2013. [Online]. Available: 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

[4] N. Perlroth, "Hackers in China Attacked The Times for Last 4 Months," *The New York Times*, January 2013. [Online]. Available: http://www.nytimes.com/2013/01/31/technology/chinese-hackers-infiltrate-new-york-times-computers.html?pagewanted=2&_r=0

[5] N. Perloth, "Washington Post Joins List of News Media Hacked by the Chinese," *The New York Times*, February 2013. [Online]. Available: http://www.nytimes.com/2013/02/02/technology/washington-posts-joins-list-of-media-hacked-by-the-chinese.html?_r=0

[6] ——, "Wall Street Journal Announces That It, Too, Was Hacked by the Chinese," *The New York Times*, January 2013. [Online]. Available: http://www.nytimes.com/2013/02/01/technology/wall-street-journal-reports-attack-by-china-hackers.html?ref=technology

[7] Human Rights Watch, "With Liberty to Monitor All: How Large-Scale US Surveillance is Harming Journalism, Law, and American Democracy," Jul. 2014, http://www.hrw.org/node/127364.

[8] K. A. Ruane, "Journalists' Privilege: Overview of the Law and Legislation in Recent Congresses," 2011. [Online]. Available: http://www.fas.org/sgp/crs/secrecy/RL34193.pdf

[9] S. Hardy, M. Crete-Nishihata, K. Kleemola, A. Senft, B. Sonne, G. Wiseman, P. Gill, and R. J. Deibert, "Targeted threat index: Characterizing and quantifying politically-motivated targeted malware," in *Proceedings of the 23rd USENIX Security Symposium*, 2014.

[10] W. R. Marczak, J. Scott-Railton, M. Marquis-Boire, and V. Paxson, "When governments hack opponents: A look at actors and technology," in *23rd USENIX Security Symposium*, 2014.

[11] S. E. McGregor, P. Charters, T. Holliday, and F. Roesner, "Investigating the computer security practices and needs of journalists," in *24th USENIX Security Symposium (USENIX Security 15)*. USENIX Association, 2015.

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

[13] C. Savage and L. Kaufman, "Phone Records of Journalists Seized by U.S." *The New York Times*, May 2013. [Online]. Available: http://www.nytimes.com/2013/05/14/us/phone-records-of-journalists-of-the-associated-press-seized-by-us.html

[14] S. Huntley and M. Marquis-Boire, "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.

[15] Freedom of the Press Foundation, "SecureDrop (formerly known as DeadDrop, originally developed by Aaron Swartz)," 2013. [Online]. Available: https://pressfreedomfoundation.org/securedrop

[16] K. Biscuitwala, W. Bult, T. J. P. Mathias Lecuyer, M. K. B. Ross, A. Chaintreau, C. Haseman, M. S. Lam, and S. E. McGregor, "Secure, Resilient Mobile Reporting," in *Proceedings of ACM SIGCOMM*, 2013.

[17] S. Carlo and A. Kamphuis, "Information Security for Journalists," The Centre for Investigative Journalism, Jul. 2014. [Online]. Available: http://www.tcij.org/resources/handbooks/infosec

[18] S. E. McGregor, "Digital Security and Source Protection for Journalists," Tow Center for Digital Journalism, Jul. 2014. [Online]. Available: http://towcenter.org/blog/digital-security-and-source-protection-for-journalists/

[19] M. Keys, "Google experts reveal how top organizations are in danger," The Blot, 2014, https://www.theblot.com/google-experts-reveal-top-organizations-danger-7717511.

[20] A. Soltani, "12 of the top 25 news sites (incl. @washingtonpost) rely on Microsoft or Google for hosted email services," Twitter, 2014, https://twitter.com/ashk4n/status/448105177439285248.

[21] P. Thornton, "Outlook/Exchange vs. GMAIL," The Journalism Iconoclast, May 2008. [Online]. Available: http://patthorntonfiles.com/blog/2008/05/26/outlookexchange-vs-gmail/

[22] N. Borisov, I. Goldberg, and E. Brewer, "Off-the-record communication, or, why not to use PGP," in *ACM Workshop on Privacy in the Electronic Society*, 2004.

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

[24] R. Dingledine, N. Mathewson, and P. Syverson, "Tor: The second-generation onion router," in *Proceedings of the 13th USENIX Security Symposium*, 2004.

[25] N. Unger, S. Dechand, J. Bonneau, S. Fahl, H. Perl, I. Goldberg, and M. Smith, "SoK: Secure Messaging," in *Proceedings of the IEEE Symposium on Security and Privacy*, 2015.

[26] M. Brennan, K. Metzroth, and R. Stafford, "Building Effective Internet Freedom Tools: Needfinding with the Tibetan Exile Community," in *7th Workshop on Hot Topics in Privacy Enhancing Technologies (HotPETs)*, 2014.

[27] Internews Center for Innovation & Learning, "Digital Security and Journalists: A SnapShot of Awareness and Practices in Pakistan," 2012, https://www.fes.de/themen/menschenrechtspreis/pdf/mrp2012/Internews.pdf.

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

[29] S. Gaw, E. W. Felten, and P. Fernandez-Kelly, "Secrecy, flagging, and paranoia: adoption criteria in encrypted email," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, 2006, pp. 591–600.

[30] G. Norcie, J. Blythe, K. Caine, and L. J. Camp, "Why Johnny Can't Blow the Whistle: Identifying and Reducing Usability Issues in Anonymity Systems," in *Workshop on Usable Security (USEC)*, 2014.

[31] A. Whitten and J. D. Tygar, "Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0," in *Proceedings of the 8th USENIX Security Symposium*, 1999.

[32] N. Diakopoulos, M. De Choudhury, and M. Naaman, "Finding and assessing social media information sources in the context of journalism," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, 2012, pp. 2451–2460.

[33] N. Taylor, D. M. Frohlich, P. Egglestone, J. Marshall, J. Rogers, A. Blum-Ross, J. Mills, M. Shorter, and P. Olivier, "Utilising insight journalism for community technology design," in *Proceedings of the 32nd ACM Conference on Human Factors in Computing Systems*. ACM, 2014, pp. 2995–3004.

[34] A. Adams and M. A. Sasse, "Users are not the enemy," *Communications of the ACM*, vol. 42, no. 12, pp. 40–46, 1999.

[35] Y.-Y. Choong and M. Theofanos, *What 4,500+ People Can Tell You - Employees' Attitudes Toward Organizational Password Policy Do Matter*, ser. Lecture Notes in Computer Science. Springer International Publishing, 2015, vol. 9190, ch. 27, pp. 299–310.

[36] K. Renaud, M. Volkamer, and A. Renkema-Padmos, "Why Doesn't Jane Protect Her Privacy?" in *Proceedings of the 2014 Privacy Enhancing Technology Symposium*, 2014.

[37] J. Corbin and A. Strauss, *Basics of qualitative research: Techniques and procedures for developing grounded theory*. Sage publications, 2014.

[38] V. Venkatesh and H. Bala, "Technology Acceptance Model 3 and a Research Agenda on Interventions," *Decision Sciences*, vol. 39, no. 2, pp. 273–315, 2008.

[39] A. Greenberg, "How the Syrian electronic army hacked us: A detailed timeline," *Forbes*, February 2014. [Online]. Available: http://www.forbes.com/sites/andygreenberg/2014/02/20/how-the-syrian-electronic-army-hacked-us-a-detailed-timeline/

[40] Symantec, "Internet security threat report 2014," 2014. [Online]. Available: http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf

[41] D. D. Caputo, S. L. Pfleeger, J. D. Freeman, and M. E. Johnson, "Going spear phishing: Exploring embedded training and awareness," *Security & Privacy, IEEE*, vol. 12, no. 1, pp. 28–38, 2014.

[42] A. Das, J. Bonneau, M. Caesar, N. Borisov, and X. Wang, "The tangled web of password reuse," in *Symposium on Network and Distributed System Security (NDSS)*, 2014.

[43] K. E. Caine, "Supporting privacy by preventing misclosure," in *CHI'09 Extended Abstracts on Human Factors in Computing Systems*. ACM, 2009, pp. 3145–3148.

[44] P. Kumaraguru, S. Sheng, A. Acquisti, L. F. Cranor, and J. Hong, "Teaching Johnny Not to Fall for Phish," *ACM Transactions on Internet Technology*, vol. 10, no. 2, pp. 7:1–7:31, Jun. 2010.

[45] PhishMe, http://phishme.com/.

[46] K. Niknejad, A. Kaphle, A. A. Omran, B. Baykurt, and J. Graham, "The New Global Journalism: Foreign Correspondence in Transition," Tow Center for Digital Journalism, Sep. 2014. [Online]. Available: http://towcenter.org/wp-content/uploads/2014/09/The-New-Global-Journalism-1.pdf