Creative and Set in Their Ways: Challenges of Security Sensemaking in Newsrooms

Elizabeth Anne Watkins
Columbia University
eaw2198@columbia.edu

Mahdi Nasrullah Al-Ameen
Clemson University
malamee@clemson.edu

Franziska Roesner
University of Washington
franzi@cs.washington.edu

Kelly Caine
Clemson University
caine@clemson.edu

Susan McGregor
Columbia Journalism School
sem2196@columbia.edu

Abstract

Maintaining computer security in an organization requires navigating a thorny landscape of adversaries, devices, and systems. As organizations grow more complex, integrating remote workers and networked, third-party tools, security risks multiply, and become more difficult to fully comprehend. News organizations are exemplary of this type of risk-laden workplace, as they combine the technical and complexity issues typical of bureaucratic systems with the creative, autonomous decision-making of journalists. As more industries face changing labor models, shifting to remote workers and building more of their computing needs on third-party platforms, journalists can serve as a critical early-warning population, a canary-in-the-coal-mine look at the management of cybersecurity in the future of work. As a first step towards building our social-science-based research, we took from organization theory the literature on sensemaking, to study how journalists who work in organizations "make sense" of cybersecurity. After analyzing interviews with a range of journalists with diverse priorities and obligations, and testing for an array of sensemaking frameworks, we found fragmented sensemaking to be pervasive. This is a hazardous condition for security in a networked organization, because such a framework correlates with misaligned and scattered behaviors. We conclude with a discussion of questions that emerged during this study, and propose next steps in research.

1 Introduction

Journalists and their organizations are high-value targets for attacks on their computer security, subject to a wide range of threats including phishing, cyberspying, and surveillance [49, 22, 1, 32]. As individuals networked together via tools of digital collaboration, including third-party document-sharing applications, cloud storage, institutional email, and content-management systems, the security behaviors of any single journalist can impact other members of their working teams and their larger organizations. Yet, our prior research [33, 34] found that journalists in such groups display asymmetry in their security behaviors, even those within established organizations. Creative, autonomous individuals bring a diverse set of obligations, motivations, and workflows into their organizations with them. Helping news institutions create effective group security practices is, then, a complex project. With the goal of drafting recommendations for these groups, we sought a framework to analyze the challenges of group-based thinking. The literature on sensemaking, in organization theory, provided a way to analyze how a group encounters and manages complex, dynamic issues like computer security.

In chaotic, dynamic situations, people must "make

sense" of events. Sensemaking is a two-step process. First, a group engages in discussion and information-sharing to graft meaning onto unanticipated, complex, or chaotic experiences. This is what happens when people have conversations, meetings, and brainstorming sessions. Second, the group then deploys these structures of meaning to make decisions about behaviors [28]. This can look like drafting strategy memos, conducting at-work training modules, and generally making recommendations for action [28]. While sensemaking is performed by any group working together to achieve a collective goal, we focus here on organizational sensemaking.

Maintaining computer security is well-suited for the sensemaking framework; it is a novel, difficult-to-comprehend, unanticipated, and influential situation [44]. We have chosen a sensemaking framework to build a foundation for studying how groups perform collective decision-making on cybersecurity. We are particularly interested in heterogenous groups, whose members hold diverse obligations, motivations, and workflows.

Prior research [9, 50] used the sensemaking framework to examine how cybersecurity is managed in groupwork. Understudied, however, is how diverse motivations, obligations, workflows, and priorities within the group impact sensemaking processes. We have a specific interest in the findings of this research, because of its implications for a variety of industries changing their labor practices, in what is broadly referred to as the "Future of Work" [8]. This shift in labor practices presents challenges to the maintenance of cybersecurity in networked organizations, especially those built atop third-party computing services. Adding more complexity to such issues are the surveillance economics underpinning many third-party communication tools, which may undermine organizational efforts to protect information.

Our work contributes granular insight, by documenting the sensemaking produced by diverse groups. Such groups will only become more common in organizations across industries, as more companies shift from traditional employment contracts to contingent, project-based, labor [8]. The portion of Americans holding contingent jobs increased from 10.1% in 2005 to 15.8% in late 2015 [26].

We used a framework for sensemaking in diverse groups to test journalists for one of four sensemaking types: guided, restricted, fragmented, and minimal. These four categories of sensemaking were first documented by organizational scholar Sally Maitlis, in her studies of working symphonies [30] and their collective decision-making processes. In designing our research, we were interested in cataloguing attributes of the organizational cybersecurity environment journalists face, to build a foundation for a body of research on this and other organizational actors.

First, we were interested in whether journalists are given cybersecurity instruction or training by their organizations (called "sensegiving"). Second, we were interested in how journalists create cognitive models of the tools and technical systems with which they engage, specifically who in their organizations they rely upon for guidance in times of ambiguity and uncertainty.

We conducted in-depth interviews with journalists about their computer security and information management practices in their professional work, and found that fewer than one-quarter of them had been instruction or guidance in security practices by their institutions. In the vacuum of sensegiving efforts on the part of organizations, we found that journalists actively engage in ad-hoc, individualized judgments, most closely resembling "fragmented sensemaking", in which many individuals concurrently make scattered, asymmetrical attempts to make sense of a chaotic situation [30]. A hazardous approach to computer security in a networked organization, such misaligned responses to attacks like spearphishing can create dangerous vulnerabilities. When considering that organizations, both private and state, are large scale custodians of data on citizens, it becomes clear that the practices by which they manage that information must be considered in larger social, legal, and policy discussions.

2 Related Work

In this section, we offer an overview of digital security threats to journalists, and an overview of prior work in the organizational literature on sensemaking.

2.1 Security and Privacy Issues in Journalism

Journalists and their organizations are subject to a range of security threats and attacks, including surveillance, spyware and malware, phishing, compromised user accounts, website defacement, and exploitation [23].

While the media's coverage of these issues often focuses on nation-state legal or technical attacks (e.g., [40, 39]), evidence suggests that less sophisticated attacks against journalists, such as phishing [22, 1] and exploitation [32], are both commonplace and on the rise [31, 25].

Due to falling revenues and increasingly powerful tools of collaboration and communication, news institutions in recent years have become more spatially distributed, structurally reorganized, and dependent on digital platforms across tasks of reporting, publishing, and measuring performance [6, 19, 47, 16].

Together with journalism's professional norms, these changes present a unique set of social, cognitive, and technical pressures on how work is conducted. Newsrooms are built to respect journalistic autonomy, especially in how reporters choose to communicate with their sources. This manifests in journalists being forced to maintain highly professional levels of skill in their technology choices, yet without any training or direction from their newsrooms: a "liquid" workflow simultaneously institutional and entrepreneurial [15, 14]. The professional norm of journalistic autonomy has been structurally codified as a pervasive failure on the part of newsrooms to provide technological (in this instance, cybersecurity) training or support.

2.2 Sensemaking

Sensemaking has received increasing attention in the HCI community in recent years [3, 7, 38, 37, 41, 36, 21], borrowing from a range of disciplines including psychology [28, 27], information and library science [13], pedagogy and teaching [5], and organizational science [30, 51, 53].

In organizational science, literature can be roughly grouped into two categories: analyses of how a group of individuals perform sensemaking collectively to respond to a crisis [29, 30, 53, 52], or examining the methods and tactics a leader uses to spearhead a group response [17, 53, 52].

2.3 Motivation: Sensemaking in Heterogeneous Groups

Missing from the literature on organizational sensemaking is an analysis of the influence wielded by stakeholders holding diverse priorities and motivations. The journalists we interviewed provided an appropriate population to test for such patterns, as prior research [33, 34] had already documented their widely divergent practices, priorities, and interests. Research on organizational sensemaking has found are four disparate patterns of sensemaking in groups of diverse stakeholders [30]:

- *Guided:* high-level managers engage in sensegiving to lower-level employees, and those employees participate in sensemaking between each other.
- *Restricted:* manager-only sensegiving, with strict controls on low-level employee activity.
- *Minimal:* little sensegiving or sensemaking on any stakeholders' part.
- *Fragmented:* little sensegiving activity from managers but animated activity between low-level employees.

A key gap is the lack of research on the motivations and priorities of lower-level stakeholders contending with an absence of leadership: while Maitlis' work [30] includes observations about the interests of high-level managers doing sensegiving, she does not document whether lower-level employees are equally diverse in their thinking. This led to our research question:

What type of security sensemaking is produced by an organizational group of diverse stakeholders, in vacuum of leadership?

This note represents early research, laying the foundation for future explorations of work groups that resemble the stakeholder makeup of journalism – groups that are diverse, creative, and autonomous in their workflows. Because this type of group will

increase in prevalence as more organizations shift to remote workers, as well as freelance, gig, and contract workers, it is critically important that we grasp the social structures which drive their security sensemaking and behaviors. The National Security Administration, it has been revealed, relies heavily on contract workers. Steve Aftergood, an intelligence analyst at the Federation of American Scientists, commented in 2013 "theres been a tremendous surge in contractor reliance, post-9/11" [4].

3 Methodology

We conducted in-depth, semi-structured interviews with 27 journalists about their computer security and information management practices in their professional work. We presented other analyses of these interviews in complementary work [34, 33]; the analysis we present here is novel.

3.1 Participants and Ethical Considerations

Our participants were employees of journalistic institutions whose primary job role could be characterized in at least one of the three categories: individual reporter, supervising (higher-level) editor, and IT professional. Journalists were not freelance, and directly employed by well-respected journalistic institutions. Journalists' primary coverage areas included investigative reporting, metropolitan beats, criminal justice, veteran's affairs and international reporting. Twelve participants were women and seventeen were men.

Participants were recruited via the authors' existing connections to journalistic institutions, usually via verbal or email contact with a staff member. Most participants were from the United States, while nine interviews were conducted in France with journalists from French and U.S. journalistic institutions. Interviews were mostly in-person, with a small portion on Skype, between November 2014 through February 2015. The entire protocol was IRB approved. Because of the potentially sensitive nature of the topic and participants, we removed all identifying information about both the journalists and their institutions during the transcription process. We explicitly asked participants not to tell us any specific or identifying information about sensitive sources or stories. Further, all data was encrypted locally before uploading to any third-party platforms, whether via email or cloud services.

3.2 Interview Script

While our interviews consisted of a range of questions about journalists' tools and practices, for this study, we focused on answers to the following specific questions:

- "Has anyone ever recommended that you use particular security technologies?"
- "Is there a resource in your organization you can go to for help?" If affirmative, the above was followed by:
- "Is that resource personal or professional?"

The first question probes for *sensegiving* on the part of the organization. The last part of the second question allowed us to identify efforts to seek out information via social connection, not from sources provided by the institution. This strategy, when deployed by members of a group, can be described as *fragmented sensemaking* [30]. The combination of these two complementary types of sensemaking allowed us to test for all four potential types of sensemaking in organizations: whether they appear discretely, in combination with each other, whether the organization actively discourages sensemaking, and whether the data display no evidence of either type.

3.3 Analysis

Following transcription of the interviews, we performed a data-driven inductive analysis [12, 46] on the text. For this analysis, the lead researcher conducted an initial and then a focused coding, identifying key indicators of sensegiving from leadership figures and fragmented sensemaking on the part of the individual journalists. The researcher then presented these themes to the entire research team, which agreed as a group on the definitions of evidence

for each theme. These themes formed the basis of a focused codebook, which was used to identify relevant text segments for analysis. Once identified, two additional team members independently coded all of the segments for all interviews. Twelve of the segments produced codes which overlapped in meaning, and so for those twelve segments a revised codebook was produced and used to recode those segments.

Evidence for sensegiving from leadership figures included accounts of:

- Organizational recommendations;
- Institutional sources of sense, such as security experts officially designated by the institution.

Evidence for fragmented sensemaking included:

- Accounts received from colleagues as opposed to leadership, including individuals or experts not officially designated by the institution but identified via social ties;
- Accounts received from external, unrelated institutional members.

Inter-rater reliability was calculated using Cohen's Kappa. Kappa has a range from 0 - 1.00. Any value of kappa over 0.75 is considered excellent agreement, with 0.40- 0.75 considered intermediate to good agreement [20].

4 Results

Our research goal is to identify what type of security sensemaking is enacted by a diverse group of workers bound together in an organization.

4.1 Sensegiving

We first tested whether or not journalists are exposed to leadership sensegiving efforts (i.e. any efforts at shaping, influencing, or guiding how employees and organizational actors both perceive and behave towards cybersecurity-related situations). We found that the majority of newsroom leaders do not engage in sensegiving in matters of computer security.

We observed a pervasive lack of cybersecurity training sessions, supporting manuals, or any regulatory attempt to control how journalists communicate with their sources.

Considering the high value of journalists as targets for cyber attack, this is surprising. Out of 21 journalists included in this portion of the study, only five (23.8%) – fewer than one-quarter – reported that their institutions engaged in sensegiving (IRR of 0.7). Some high-level editors and technologists spoke directly to the problem of enacting sensegiving in their institutions:

> The biggest challenge in the newsroom is that you're consistently herding cats. Your basic compliance, getting a herd of journalists to all do something ... is a management challenge, a tough thing to do with the crowd of people we're dealing with: they're creative, they're kind of set in their ways. To get them to change everything would be an achievement. (E4)

> It's a challenge because reporters like to use their own stuff, and in terms of our IT folks, I don't envy the battle they have. (T5)

> For security tools a lot of times it just feels like an extra layer that people don't want to deal with. ... getting everyone on board is really hard for a large organization. (E2)

Rather than create organizational mandates about security, newsrooms instead instructed journalists to make their own judgment in conversation with their sources, based on their their technical options, their specific vulnerabilities, and their workflows.

4.2 Sensemaking

We found that the vacuum of leadership correlated with highly animated employee activity: a majority of the respondents (n=18, 66.7%) reported that they had deliberately identified people they could turn to for assistance in times of confusion. In our breakdown of this group of "guides," we found a surprising split. While eight of our participants noted that their guide was an institutionally designated individual, ten respondents (37.0%) reported that their source of guidance was a social contact or friend – people whose advice institutional leaders can neither evaluate nor control.

This type of sensemaking can be catalogued as "fragmented," in which collaborators simultaneously make asymmetrical, ad-hoc, individualized attempts to make sense of a chaotic situation. This individual action pattern has been shown to correlate with group actions that are uncontrolled, multiple, narrow, and inconsistent [30].

This is a particularly hazardous approach to computer security in a networked organization, as misaligned responses to such attacks like spearphishing can create dangerous vulnerabilities not just for individuals, but for the while organization.

To protect anonymity, individual journalists' particular beats were not recorded alongside their responses. Some high-level editors, however, volunteered coverage beat or type as a driving motivator for the cybersecurity-oriented choices they made for their teams:

> We tend to work on more sensitive stories, so information security is a primary issue that we have. (E1)

> [Training is] handled kind of on an ad-hoc basis by different reporters and teams depending on the sensitivity of the kind of stories they're working on. (E3)

This ad-hoc, beat-dependent attitude towards security has been found to exist among reporters as well. For example, prior work indicates that lower-level journalists sort themselves into vulnerability categories determined by the perceived sensitivity of a given beat or story:

> If you were on the national security beat [security technology] would be really useful. But I write about domestic social problems, education, crime, poverty. [35]

Such behaviors seem to reflect the type of advice journalists also provide to one another. For example, a self-described investigative journalist who had experienced a physical security breach had articulated his type of work, indicating a perceived correlation between his beat as an investigative reporter, his threat landscape, and the concerns of his peers.

> Everyone tells me to be careful. During the time I was being surveilled, my house was burgled, and my computer was stolen – just my computer. So since then Ive been very careful. ... this is why I encrypt things and installed an alarm system in my home. (P6)

Though his personal experience of a security breach appears correlated with subsequent behavior changes on his part (i.e. the adoption of encryption practices and an alarm device), it is unclear whether these particular actions were prompted by his own reaction to the breach, or by the advice he received from colleagues.

5 Conclusion

News organizations offload security decisions to journalists and sources. Because journalists' professional authority and economic livelihood depends on creating an efficient and comfortable infrastructure for information-transfer from sources, they allow their sources to dictate their security practices:

> [The source] probably understand[s] the threat model theyre under better than I would. So, it brings up an interesting question: do you go with what theyre comfortable with? Or do you say, alright, actually let me assess whats going on and get back to you with what would be appropriate. [...] Peoples first impression is that they would go by what the source feels comfortable doing. [33]

This source-based approach to cybersecurity, however, has already been observed to be a poor match for the actual technical dangers faced by journalistic organizations, while many of the threats faced by journalists are from spearphishing attacks. These get inside an organization by targeting anyone in that organization, regardless of who their sources are or how sensitive their information is. There is a mismatch, then, between the threat models that journalists glean from sources, and the actual technological environment they inhabit. In our related work, we found that this pattern persisted across both reporters and editors, despite the fact that editors knew details around specific security incidents that did not

support a relationship between particular reporter beats and security risk [33].

In delegating security decisions to journalists, newsroom foster an environment in which journalists actually act against their own interests. Newsrooms' information management practices force journalists to create and deploy their own mental models of cybersecurity, often based on making information-transfer infrastructures comfortable and efficient for sources.

Encouraging this type of ad-hoc strategy leads to a spread of misinformation, perpetuating a balkanized, confused security landscape. Additional dangerous results coming out of this lack of unified mandate can be found in a 2015 Pew Research survey of journalists, which found that 50% of them had not used any of the eight widely used tools of encryption shown to them [24]. As we see, this scattered organizational approach to computer security presents hazardous vulnerabilities; misaligned behaviors in this space can introduce dangers not just to individuals, but to the whole organization.

6 Discussion

Our findings parallel prior research showing that social learning heavily influences security-related decisions [11], and that the security recommendations that people hear from friends have notable impact on their security beliefs and behavior [42]. A 2010 survey of 333 American citizens showed that informal discussions about security awareness with work colleagues, in particular, was preferred as a source of learning, even over formal at-work training [45]. From these studies, we wonder whether the interaction of social sensemaking and the work environment may be a key site for gaining security awareness.

In a larger research agenda, we are interested in building on this and other studies examining the human factors of cybersecurity, especially in networked organizations engaging in so-called "future of work" practices. Specifically 1) remote or distributed work models, including freelance, gig, and 1099 labor, and 3) the use of cloud computing.

At the Global Leadership summit held in London in 2014, 34% of business leaders surveyed said more than half of their company's full-time workforce would work remotely by 2020 [48]. As of 2017, 43% of working Americans spend some at least some portion of their time working remotely - an all-time high [10]. When we consider the influential role played by social sensemaking, both in our research and in the literature, it seems worth investigating whether remote or contract workers' lower rate of exposure to social processes, i.e. lack of proximity to sites of shared learning [18], impacts their behaviors. How will the loss of social influence, which is shown to be significant in the transmission of security sensemaking, operate in disconnected work environments? Even in the event that formal training is provided to all workers regardless of their status, freelance workers may be less inclined to access cybersecurity training. We found early evidence for this in our own interviews. One of our participants mentioned this vulnerability specifically:

> Many of our writers are not staff. They're contract/freelance - both contract and freelance. We have some contractors who have regular spots - you know, they write one column a week, but they're not employees and they never come into either of our offices. They would be invited to participate [in a training session, but], they likely would not. (T3)

How would such a condition, where remote/contract workers don't access cybersecurity training, impact communities who rely on gig platforms for work opportunities? Future research is needed to examine how work environments and social sensemaking interact to influence security awareness. Our research agenda includes surveying the greater public to assess where their most salient security lessons have originated, and the role played by at-work sensemaking practices. We also plan to conduct interviews with contingent workers across industries. Will cybersecurity knowledge become a luxury good, reserved for the few who still engage with their organizations via traditional employment contracts?

Also of interest to us are the challenges presented

by the growing prevalence of third-party vendor tools, cloud computing, and Software-as-a-Service products. The introduction of remote servers, devices, and even legislative contexts (if a server is based across state boundaries) introduces novel security vulnerabilities into a networked ecosystem. Further, more services becoming off-loaded to "the cloud" may present a hurdle to sensemaking. Users have been observed building mental models of information systems to make decisions about their cybersecurity behaviors, and such systems may become more difficult to fully understand as they become more dispersed. For example, many of our participants expressed concern about storing sensitive information on collaborative work platforms like Google Docs, indicating an awareness that putting data on remote servers may make it vulnerable to hacks or subpoenas on the host firm. However, one participant, just minutes after expressing such awareness, voiced a wish for better Google transcription services, seemingly unaware that using such services also copies that data onto Google's servers. Future research on our agenda addresses the use of such third-party services in newsrooms.

One industry of particular interest is the financial services sector. Client data protection mandates set by the Securities and Exchange Commission's 2015 Cybersecurity Examination Initiative subjects firms to liability if they fail to take steps to prevent cyberattacks [43]. The Office of Compliance Inspections and Examinations has specifically referenced vulnerabilities presented by vendor software: "Some of the largest data breaches over the last few years may have resulted from the hacking of third party vendor platforms" [2].

In this paper, our data-driven contribution is twofold: first, we have identified the type of sensemaking that journalists, a type of diverse organizational group who are "creative and set in their ways" performs. Second, we have described what structural elements of these organizations contribute to these security practices.

In terms of actionable recommendation, and the observed salience of shared learning and storytelling, organizations could benefit from leveraging more "organic" social sensemaking activities. Employees could be encouraged to share stories of hacks or data breaches they have experienced. Managers could collect news stories of data breaches that similar firms have experienced and share them with their employees. If a firm experiences a breach or attack, implementing a mandate of follow-up community discussion could function as a type of postmortem exercise, similar to those undertaken in the medical field after the death of a patient [50].

Alternatively, organizations could tailor their training to better reflect the threat landscapes faced. Because newsworkers are subject to spearsphishing, for example, workplaces could implement "test" emails to gauge the savvy of their workers. A curious click on an unsecure link could trigger a warning and a reminder. We plan to validate these recommendations through future studies.

In a larger, theory-driven contribution, we argue that we need to understand sensemaking in news organizations for two reasons: first, to better protect journalists and their sources in a fraught environments, and second, to better theorize how organizations across industries manage cybersecurity. As many organizations grow their data depositories, from social-media platforms to finance to healthcare, the way these companies instruct their employees to handle our data has critical implications for broader economic, social, and legal discussions.

As one editor in our study put it:

> [Security training is] not part of the onboarding - it's cultural communication. (T3)

References

[1] 2013. Hackers compromise AP Twitter account. *Associated Press.* http://bigstory.ap.org/article/hackers-compromise-ap-twitter-account. (April 2013).

[2] 2015. Guidance Update. (April 2015). https://www.sec.gov/investment/im-guidance-2015-02.pdf.

[3] Ann Abraham, Marian Petre, and Helen Sharp. 2008. Information seeking: Sensemaking and interactions. *City* (2008).

[4] Spencer Ackerman. 2013. Snowden leak shines light on US intelligence agencies' use of contractors. (Jun 2013). https://www.theguardian.com/world/2013/jun/10/edward-snowden-booz-allen-hamilton-contractors.

[5] Florence Allard-Poesi. 2005. The paradox of sensemaking in organizational analysis. *Organization* 12, 2 (2005), 169–196.

[6] C.W. Anderson, E. Bell, and C. Shirky. 2013. Post-Industrial Journalism: Adapting to the Present. (2013). http://towcenter.org/research/post-industrial-journalism-adapting-to-the-present-2/.

[7] Simon Attfield, Ann Blandford, and D de Gabrielle. 2008. Investigations within investigations: a recursive framework for scalable sensemaking support. (2008).

[8] Stephen Barley, Beth Bechky, and Frances Milliken. 2017. FROM THE EDITORS: The Changing Nature of Work: Careers, Identities, and Work Lives in the 21st Century. *Academy of Management Discoveries* (2017), amd–2017.

[9] Jeffrey M Bradshaw, Marco Carvalho, Larry Bunch, Tom Eskridge, Paul J Feltovich, Chris Forsythe, Robert R Hoffman, Matt Johnson, Dan Kidwell, and David D Woods. 2015. Coactive Emergence as a Sensemaking Strategy for Cyber Security Work. (2015).

[10] Niraj Chokshi. 2017. Out of the Office: More People Are Working Remotely, Survey Finds. The New York Times. (2017). https://www.nytimes.com/2017/02/15/us/remote-workers-work-from-home.html.

[11] Nicola Davinson and Elizabeth Sillence. 2014. Using the health belief model to explore users' perceptions of 'being safe and secure' in the world of technology mediated financial transactions. *International Journal of Human-Computer Studies* 72, 2 (2014), 154–168.

[12] Jessica T DeCuir-Gunby, Patricia L Marshall, and Allison W McCulloch. 2011. Developing and using a codebook for the analysis of interview data: An example from a professional development research project. *Field methods* 23, 2 (2011), 136–155.

[13] Brenda Dervin, Lois Foreman-Wernet, and Eric Lauterbach. 2003. *Sense-making methodology reader: Selected writings of Brenda Dervin*. Hampton Pr.

[14] Mark Deuze. 2008. The changing context of news work: Liquid journalism and monitorial citizenship. *International Journal of Communication* 2, 5 (2008), 848–865.

[15] Mark Deuze and Tamara Witschge. 2017. Beyond journalism: Theorizing the transformation of journalism. *Journalism* (2017), 1464884916688550.

[16] Nicholas Diakopoulos. Computational Journalism and the Emergence of News Platforms. (????).

[17] Tobias Dyrks, Sebastian Denef, and Leonardo Ramirez. 2008. An empirical study of firefighting sensemaking practices to inform the design of ubicomp technology. In *Sensemaking Workshop of the SIGCHI Conference on Human Factors in Computing Systems (CHI 2008). Retrieved from http://dmrussell. googlepages. com/Dryks-final. pdf.*

[18] Thomas Erickson and Wendy A Kellogg. 2000. Social translucence: an approach to designing systems that support social processes. *ACM transactions on computer-human interaction (TOCHI)* 7, 1 (2000), 59–83.

[19] Sandra K. Evans. 2016. Staying Ahead of the Digital Tsunami: The Contributions of an Organizational Communication Approach to Journalism in the Information Age. *Journal of Communication* 66, 2 (2016), 280–298. DOI:http://dx.doi.org/10.1111/jcom.12217

[20] Joseph L Fleiss, Bruce Levin, and Myunghee Cho Paik. 2013. *Statistical methods for rates and proportions*. John Wiley & Sons.

[21] Nitesh Goyal and Susan R Fussell. 2015. Designing for Collaborative Sensemaking: Leveraging Human Cognition For Complex Tasks. *arXiv preprint arXiv:1511.05737* (2015).

[22] Andy Greenberg. 2014. How The Syrian Electronic Army Hacked Us: a detailed timeline. *Forbes website, available at¡ http://www. forbes. com/sites/andygreenberg/2014/02/20/how-the-*

syrian-electronic-army-hacked-us-a-detailed-timeline/¿ accessed 30 (2014).

[23] Jennifer R Henrichsen, Michelle Betz, and Joanne M Lisosky. 2015. *BUILDING DIGITAL SAFETY FOR JOURNALISM.* United Nations Educational, Scientific and Cultural Organization.

[24] Jesse Holcomb, Amy Mitchell, and Kristen Purcell. 2015. Adoption of Digital Security Tools. (Feb 2015). http://www.journalism.org/2015/02/05/adoption-of-digital-security-tools/.

[25] Jason Hong. 2012. The State of Phishing Attacks. *Commun. ACM* 55, 1 (Jan. 2012), 74–81. DOI:http://dx.doi.org/10.1145/2063176.2063197

[26] Lawrence F Katz and Alan B Krueger. 2016. *The rise and nature of alternative work arrangements in the United States, 1995-2015.* Technical Report. National Bureau of Economic Research.

[27] Gary Klein, Brian Moon, and Robert R Hoffman. 2006a. Making sense of sensemaking 2: A macrocognitive model. *IEEE Intelligent Systems* 21, 5 (2006), 88–92.

[28] Gary Klein, Brian M Moon, and Robert R Hoffman. 2006b. Making Sense of Sensemaking 1: Alternative Perspectives. *IEEE intelligent systems* 21, 4 (2006), 70–73.

[29] CP Lee and S Abrams. 2008. Group sensemaking. In *CHI 2008 Sensemaking Workshop. Florence, Italy.*

[30] Sally Maitlis. 2005. The social processes of organizational sensemaking. *Academy of Management Journal* 48, 1 (2005), 21–49.

[31] Mohammad Mannan, Tara Whalen, Robert Biddle, and PC van Oorschot. 2010. *The usable security of passwords based on digital objects: From design and analysis to user study.* Technical Report. Technical Report TR-10-02, School of Computer Science, Carleton University.

[32] N. Mattise. 2014. Syrian electronic army targets Reuters again but ad network provided the leak. *ArsTechnica* (June 2014).

[33] Susan E McGregor, Polina Charters, Tobin Holliday, and Franziska Roesner. 2015. Investigating the computer security practices and needs of journalists. In *24th USENIX Security Symposium (USENIX Security 15).* 399–414.

[34] Susan E McGregor, Franziska Roesner, and Kelly Caine. 2016. Individual versus Organizational Computer Security and Privacy Concerns in Journalism. *Proceedings on Privacy Enhancing Technologies* 4 (2016), 1–18.

[35] Susan E McGregor and Elizabeth Anne Watkins. Security by Obscurity: Journalists Mental Models of Information Security. (????).

[36] Les Nelson, Christoph Held, Peter Pirolli, Lichan Hong, Diane Schiano, and Ed H Chi. 2009. With a little help from my friends: examining the impact of social annotations in sensemaking tasks. In *Proceedings of the SIGCHI conference on human factors in computing systems.* ACM, 1795–1798.

[37] Sharoda A Paul and Meredith Ringel Morris. 2009. CoSense: enhancing sensemaking for collaborative web search. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems.* ACM, 1771–1780.

[38] Sharoda A Paul and Meredith Ringel Morris. 2011. Sensemaking in collaborative web search. *Human–Computer Interaction* 26, 1-2 (2011), 72–122.

[39] Nicole Perlroth. 2013a. Hackers in China attacked The Times for last 4 months. *NY Times, Jan* 30 (2013).

[40] Nicole Perlroth. 2013b. Washington Post joins list of news media hacked by the Chinese. *The New York Times* 1 (2013).

[41] Peter Pirolli and Daniel M Russell. 2011. Introduction to this special issue on sensemaking. *Human–Computer Interaction* 26, 1-2 (2011), 1–8.

[42] Emilee Rader, Rick Wash, and Brandon Brooks. 2012. Stories as informal lessons about security. In *Proceedings of the Eighth Symposium on Usable Privacy and Security.* ACM, 6.

[43] Brian Rubin, Brian Rubin, Amy Xu, and Amy Xu. 2016. Cybersecurity enforcement actions: is the SEC bringing strict liability cases? *Journal of Investment Compliance* 17, 1 (2016), 112–116.

[44] Nikhil Sharma and George Furnas. 2009. Artifact usefulness and usage in sensemaking handoffs. *Proceedings of the American Society for Information Science and Technology* 46, 1 (2009), 1–19.

[45] Shuhaili Talib, Nathan L Clarke, and Steven M Furnell. 2010. An analysis of information security awareness within home and work environments. In *Availability, Reliability, and Security, 2010. ARES'10 International Conference on*. IEEE, 196–203.

[46] David R Thomas. 2006. A general inductive approach for analyzing qualitative evaluation data. *American journal of evaluation* 27, 2 (2006), 237–246.

[47] N. Usher. 2014. *Making News at The New York Times*. University of Michigan Press, Ann Arbor, Michigan.

[48] Laura Vanderkam. 2014. Will Half Of People Be Working Remotely By 2020? *Fast Company* (Aug 2014). `https://www.fastcompany.com/3034286/will-half-of-people-be-working-remotely-by-2020`.

[49] Jeremy Wagstaff. 2014. Journalists, media under attack from hackers: Google researchers. (March 2014). http://www.reuters.com/article/us-media-cybercrime-idUSBREA2R0EU20140328.

[50] Elizabeth Anne Watkins, Franziska Roesner, Susan McGregor, Byron Lowens, Kelly Caine, and Mahdi Nasrullah Al-Ameen. 2016. Sensemaking and Storytelling: Network Security Strategies for Collaborative Groups. In *Collaboration Technologies and Systems (CTS), 2016 International Conference on*. IEEE, 622–623.

[51] Karl E Weick. 1995. *Sensemaking in organizations*. Vol. 3. Sage.

[52] Karl E Weick. 2005. 5 Managing the Unexpected: Complexity as Distributed Sensemaking. In *Uncertainty and surprise in complex systems*. Springer, 51–65.

[53] Karl E Weick, Kathleen M Sutcliffe, and David Obstfeld. 2005. Organizing and the process of sensemaking. *Organization science* 16, 4 (2005), 409–421.