Security and Privacy Perception of Sources Who Discussed Sensitive Topics with Journalists

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

Byron Lowens
Clemson University
blowens@g.clemson.edu

Susan Mcgregor
Columbia Journalism School
sem2196@columbia.edu

Kelly Caine
Clemson University
caine@clemson.edu

ABSTRACT

In recent years, journalist-source communications have been the major target of cyber attacks and state-sponsored surveillance. We conducted an online survey to investigate into the security perception of sources who discussed sensitive topics with journalists, in terms of their awareness of digital surveillance and relevant privacy issues. Our results showed that only a handful of sources discussing sensitive topics, used secure tools during their communication with journalists, where we identified gaps between their security awareness and practices, and revealed their lack of confidence in finding secure tools and protecting sensitive information. Our study demonstrated the importance of bringing together journalists and information security specialists, to develop security training modules tailored to the needs of journalists. We documented the demographic factors to be considered in developing such training to improve securing and privacy in journalism.

Keywords

Security perception; Journalistic sources; Online survey

1. INTRODUCTION

Journalist-source communications are targets of computer security attacks because of the type, value, and temporally sensitive nature of information that they communicate. While users are often considered to be the weakest link in computer security, developing solutions and practices to protect these communications demands that we understand the unique perspective of both journalists [16] *and* their sources.

The common types of computer security attacks documented against journalists include hacking, phishing, spyware, denial of service, and exploitation (e.g., compromised router hardware) [8]. In recent years, 21 of the world's top-25 news organizations have been the target of hacking attacks [24]; several prominent US news organizations including The New York Times, The Wall Street Journal, Bloomberg, and The Washington Post revealed that they had been the targets of state-sponsored digital attacks designed to identify journalists' sources [17, 18]. As another example, Ethiopian Satellite Television Service (ESAT) employees were attacked with sophisticated computer spyware designed to steal secret credentials, and intercept Skype calls and instant messages [13].

Motivations. Evidence suggests that many of these attacks and surveillance targeted journalists who report on sensitive topics [7, 14, 19], which call into the question journalists' ability to protect their sources [12], and have led to a documented "chilling effect" that can result in sources reducing or terminating communication with journalists [15]. Indeed, the freedom of the press to report on topics of public concern is threatened, if sources cannot trust that their identities and communications with journalists will be protected.

While prior research [2, 9, 15, 23] studied the security perception and practices of professional journalism community, similar work has not been done yet for their sources, despite the fact that sources could discuss sensitive topics with journalists and play an integral role in choosing the communication tools used for journalism [15]. Thus, it is imperative to understand the sources' needs and concerns around secure communication technologies, specially when they discuss sensitive topics with journalists [1]. We addressed this challenge in our research.

Contributions. In our online survey on 621-U.S.-based participants (580 data were usable), 76 participants reported that they had communicated with members of the media and discussed sensitive topics during their interaction with journalists. However, only 12 of that 76 sources used secure communication tools, where we identified gaps between their security awareness and practices. We explored the security perception of sources in terms of their awareness of government surveillance and relevant privacy issues, which reveals their lack of confidence in finding secure tools and protecting sensitive information. Our recommendations include focusing on security training and education for secur-

[1] A recent study [15] identified that news stories related to the topics listed in Table 2, are generally considered *sensitive* by the journalists.

ing journalist-source communication, where we documented the demographic factors to be considered in developing such training.

2. METHOD

In this section, we describe the content, platform, and procedure of our study.

Survey Content and Platform. Our survey consisted of the questions to understand whether the participants acted as a source, discussed sensitive topics with journalists [1], and how they conducted these communications. We also asked participations about their demographics, and privacy and security perception. Attention checks were distributed throughout the survey to ensure data quality.

We recruited participants through Amazon Mechanical Turk (MTurk), a crowd-sourcing web service that manages the supply and demand of tasks requiring human intelligence to complete, which has emerged as a prominent platform for experimental and survey-based academic research because of the diversity and representativeness of sample workers [11].

Procedure. The survey instrument was implemented in Qualtrics [2]. The advertisements on MTurk presented the purpose of our study, procedures, anticipated completion time, and compensation. We provided participants a link to complete the Qualtrics survey via MTurk. Participants were compensated with $1.00 for completing the survey, and those who had communicated with a member of the media earned a bonus of $4.00 due to the additional time required to answer the questions on their communication with journalists. The entire study was reviewed and approved by our Institutional Review Board.

Prior to participation in the survey, participants were asked to read an informed consent document. During this time, we also informed participants that they would only receive payment if they could successfully pass attention checks throughout the survey. Because U.S. MTurk workers often seek anonymity and have a profound concern for privacy [11], we did not collect identifying information such as names in connection with survey responses.

3. RESULTS

In this section, we report the findings from our study. We deployed the survey to 621 U.S.-based participants from all 50 states plus the District of Columbia, where 580 participants passed all of the attention check questions. Among them, 76 participants reported that they had communicated with members of the media and discussed sensitive topics during their interaction with journalists. We considered these 76 participants for our analysis, and note them as *sources* in the rest of the paper, unless otherwise specified.

As reflected in Table 1, out of that 76 sources in our study, half of them are female, above 80% of them are white, and two-third of them were in the age range of 25-44. Most of the sources (96%) had at least some college degree, with 60% of them having at least a 4-year college degree.

Sensitive topics, like *personal information not to be mentioned* and *vulnerable populations* were discussed by most number of sources, in particular, by 54% and 51% of sources, respectively (see Table 2).

[2]Qualtrics is an online survey platform used to create, distribute, collect, and analyze survey data (`www.qualtrics.com`).

Table 1: Demographics of Sources (N=76)

Demographics	% of sources
Gender	
Male	50%
Female	50%
Age-range	
18-24	9%
25-34	45%
35-44	21%
45-54	13%
55-64	8%
65+	4%
Race/Ethnicity	
White	82%
Black or African American	11%
Asian or Asian American	1%
Hispanic/Latino	4%
Other	3%
Education	
High school incomplete or less	0%
High school graduate or GED	4%
Some College	36%
Four Year College Degree	39%
Some postgraduate or professional schooling	5%
Post graduate	16%

Table 2: Sensitive Topics

Sensitive Topics	% of sources N = 76
Personal information not to be mentioned	54%
Vulnerable populations	51%
Off the record by government officials	30%
Leaked or stolen documents	20%

3.1 Communication Methods

As shown in Table 3, email, in-person, telephone, and social media are the most common interaction methods between journalists and sources. We found that 80% of sources used email as the communication medium, where 12% of sources used encrypted email. Similarly, with 70% of sources using telephone, only 5% of sources used encrypted phone for communicating with journalists. 21% of sources used Dropbox to share documents, where 8% of sources used SecureDrop, a document sharing tool designed for secure communication between journalists and sources [6].

Overall, 84% of sources never used any kind of secure tools during their communication with journalists. The average number of journalists a source communicated with is 8, while the sources who used secure communication tools communicated with 14 journalists, on average. Above half of the sources (57%) never requested anonymity during their interaction with journalists.

Table 3: Interaction Methods

Regular Communication	**% of sources** N = 76	**Secure Communication**	**% of sources** N = 76
Email	80%	Encrypted Email	12%
In-person	71%	Encrypted Chat	9%
Telephone	70%	Encrypted Messaging	8%
Social Media	64%	SecureDrop	8%
Letter	38%	VPN	7%
Chat	36%	Absio Dispatch	7%
Video Chat	33%	Encrypted Phone	5%
SMS	29%	TOR	4%
Google Docs	22%	Other Encryption	4%
Dropbox	21%	Other	4%
Evernote	16%	-	
Scrivener	13%	-	
Other	7%	-	

Table 4: Protecting Personal Information Online

Protecting Personal Information Online	**% of Sources** N = 76
Already Did Enough	30%
Would like to do more	70%
Prefer not to answer	0%

Table 5: Ability to use Internet Anonymously

Ability to use Internet Anonymously	**% of Sources** N = 76
Should be able to	71%
Should not be able to	26%
Prefer not to answer	3%

Table 6: Awareness of Government Surveillance

Awareness of Govt. Surveillance	**% of Sources** N = 76
A lot	53%
A little	38%
Nothing at all	7%
Do not know	3%
Prefer not to answer	0%

Table 7: Concern about Government Surveillance

Concern about Gov't Surveillance	**% of Sources** N = 76
Very concerned	36%
Somewhat concerned	0%
Not at all concerned	64%
Do not know	0%
Prefer not to answer	0%

Out of that 12 sources who used secure communication tools, 4 are female and 8 are male, who are in the age-range of 18-44. As we found, 15% of sources in the age-range of 18-24, 18% of sources in the age-range of 25-34, and 31% of sources in the range of 35-44 used secure tools during their communication with journalists. In terms of education, the sources using secure communication tools had at least some college degree, where 15% of sources who attended some college (e.g., two year college degree), 20% of sources who had four year college degree, and 50% of sources who had some post-graduate or professional schooling, used secure tools while communicating with journalists.

3.2 Security and Privacy Perception

In this section, we present our results on the security and privacy perception of sources, where we also identified the gaps with their security practices, that the research community should address to improve security and privacy in journalist-source communication.

3.2.1 Gap between security perception and practices

In response to the question: "Do you feel as though you already did enough to protect the privacy of your personal information online, or do you feel as though you would like to do more?", about one-third (30%) of sources felt they had already done enough (see Table 4), despite low adoption of secure communication tools: only four of them used secure tools during their communication with journalists.

In response to the question: "Do you think that people should have the ability to use the Internet completely anonymously for certain kinds of online activities?", 71% of sources gave response that people should be able to use the Internet anonymously (see Table 5). However, a very few of that 71% sources reported using anonymous communication tools: two of them used both TOR and SecureDrop, and four of them used only SecureDrop during their interaction with journalists.

3.2.2 Gap between security awareness and practices

In response to the question: "How much, if anything, have you heard about the government collecting informa-

Table 8: Finding Security Tools and Strategies

Finding Security Tools and Strategies	**% of Sources** N = 76
Very easy	9%
Somewhat easy	49%
Somewhat difficult	28%
Very Difficult	13%
Do not know	1%
Prefer not to answer	0%

Table 9: Difficulty in Uncovering Sensitive Information

Difficulty in Uncovering Sensitive Information	**% of Sources** N = 76
Very difficult	3%
Somewhat difficult	33%
Not too difficult	34%
Not at all difficult	28%
Do not know	3%
Prefer not to answer	0%
Not Applicable	0%

tion about telephone ca1ls, emails, and other online communications as part of efforts to monitor terrorist activity?", above half (53%) of the sources noted that they had heard "a lot" about government surveillance (see Table 6). However, among that 53% of sources who reported to be well aware of government surveillance, only 5 (13%) of them used secure communication tools, and 15 (38%) of them requested anonymity during their interaction with journalists.

We also found gap between security concern and practices of sources. In response to the question: "Overall, how concerned are you about government surveillance of Americans' data and electronic communications", above one-third (36%) of sources reported to be "very concerned" about this issue (see Table 7), however, among them, only 3 (11%) sources used secure communication tools, and 10 (37%) sources requested anonymity while communicating with journalists.

3.2.3 Lack of confidence in finding secure tools and protecting sensitive information

In response to the question, "If you wanted to be more private while you were using the Internet or your cell phone, how easy do you think it would be for you to find tools and strategies that would help you?", only 9% of sources reported it to be "very easy", where 41% of sources reported that it would be "somewhat difficult" or "very difficult" to find secure communication tools and strategies (see Table 8).

In response to the question: "If a motivated person or organization wanted to learn details about your past that you would prefer to keep private, how difficult do you think it would be for them to uncover that sensitive information?", only 2 (3%) sources reported that it would be "very difficult", where a majority (62%) of sources reported that it would be "not too difficult" or "not at all difficult" for a motivated entity to uncover sensitive information from the past (see Table 9).

4. DISCUSSION

In this section, we discuss about the implications of our findings, and identify the scopes of future research.

4.1 Security Practice and Perception

Our study identified email and telephone as two of the top three most commonly used medium for journalist-source communication. However, a small fraction of sources used them in a secure (i.e., encrypted) way, while insecure use of these technologies have put journalists and their sources increasingly at risk of identification, prosecution, and persecution by powerful entities. Recent examples of such threats include the secret seizure of journalists' phone records by the U.S. Justice Department [21] and the collection of journalists' emails by the British intelligence agency GCHQ [1].

Security practice of users is motivated by their perception, awareness, and concern [3, 10, 20]. However, our findings yield gaps between security practices of sources and their security perception, awareness, and concern: although above half of the sources are well-aware of government surveillance, very few of them used secure tools during their interaction with journalists. Similarly, with above two-third of sources reporting the importance of maintaining anonymity during certain online communications, most of them did not use any type of anonymous communication tools (e.g., TOR, SecureDrop). Below, we present a deeper insight into these gaps between security perception and practices.

Users' perceived level of security threat remains low when they think it to be unlikely of being a victim of digital attacks [4], i.e., people possess a tendency to care less about "distant" harms [5], where personal experience — for example, being a victim of the cyber attack motivates users to change their security practice [5]. It could also explain our findings why a fraction of sources felt that they had already done enough to protect their online privacy, despite low adoption of secure communication tools.

Our results indicated lack of confidence among sources in protecting their sensitive information and finding security tools to ensure online privacy, which is another possible reason behind the gaps between their security awareness and practices.

We also identified that for many sources, their awareness of government surveillance did not translate into concern, and thus, might not have motivated them to adopt secure communication tools. For example, among that sources who had heard "a lot" about government surveillance, around 45% of them reported to be "not at all concerned" about this issue. The reduced sense of responsibility for any negative outcomes could be a lead factor for such mental model of users [4].

In our study, very few sources reported using security tools developed specifically for journalists, such as SecureDrop that supports anonymous document sharing [6]. Our findings are in line with that from prior study [15], which also reported low adoption rate of SecureDrop among journalists, and identified the usability challenges of using this tool for journalist-source communication. So, the unsatisfactory usability of the existing security tools might also contribute to the low adoption rate of secure communication technologies among sources.

4.2 Security Training and Education

We found that no user, who did not attain at least some

college degree, used secure tools for communicating with journalists. So, the general education might have relation to the overall security consciousness. However, the rate of using secure communication tools is still quite low among the educated users. Thus, there exists a gap between general and security education, which points to the necessity of finding effective strategies of blending security training into general education curriculum.

The prior study [22] reported that female users are more vulnerable, as compared to male users, to digital attacks including phishing. In our study, while half of the sources are female, 4 of them used secure communication tools that is half of the number of male sources (8) using secure tools while communicating with journalists. Also, the sources who were above 44 years old (one-fourth of all sources), did not use any secure technologies during their interaction with journalists. Thus, future research should identify the measures that security educators should adopt to make female and older users more conscious of using secure tools and strategies to protect against cyber attacks.

5. CONCLUSION

In this paper, we presented the security and privacy perception of sources who discussed sensitive topics with journalists. Our analysis revealed their awareness of government surveillance and relevant privacy issues, offering deeper insights into the gaps between their security perception and practices. We also identified a gap between general and security education, pointing to the importance of bringing together journalists and information security research community, to develop effective security training and education focused on journalism. As we identified the importance of considering demographic factors while designing such training, the future research should investigate deeper into these issues.

6. REFERENCES

[1] J. Ball. Gchq captured emails of journalists from top international media. *The Guardian, Jan*, 2015.

[2] M. Brennan, K. Metzroth, and R. Stafford. Building more effective internet freedom tools: Needfinding with the tibetan exile community. 2014.

[3] J. Chen, M. Paik, and K. McCabe. Exploring internet security perceptions and practices in urban ghana. In *SOUPS*, pages 129–142, 2014.

[4] N. Davinson and E. Sillence. 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):154–168, 2014.

[5] P. Dolan, M. Hallsworth, D. Halpern, D. King, and I. Vlaev. Mindspace: influencing behaviour through public policy [internet]. london: Institute for government; c2010, Accessed: March 31, 2012.

[6] Freedom of the Press Foundation. SecureDrop (formerly known as DeadDrop, originally developed by Aaron Swartz), 2013.

[7] A. Greenberg. 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.

[8] J. R. Henrichsen, M. Betz, and J. M. Lisosky. *BUILDING DIGITAL SAFETY FOR JOURNALISM*. United Nations Educational, Scientific and Cultural Organization, 2015.

[9] J. Holcomb, A. Mitchell, and K. Purcell. Investigative journalists and digital security. *Pew Research Center. http://www. journalism. org/2015/02/05/investigative-journalists-and-digital-security year=2015*.

[10] I. Ion, R. Reeder, and S. Consolvo. "... no one can hack my mind": Comparing expert and non-expert security practices. In *Eleventh Symposium on Usable Privacy and Security (SOUPS 2015)*, pages 327–346, 2015.

[11] R. Kang, S. Brown, L. Dabbish, and S. B. Kielser. Privacy attitudes of mechanical turk workers and the us public. In *SOUPS*, pages 37–49, 2014.

[12] C. F. Kleberg. The death of source protection? protecting journalists' source in a post-snowden age. 2015.

[13] B. Marczak, C. Guarnieri, M. Marquis-Boire, and J. Scott-Railton. Hacking team and the targeting of ethiopian journalists. *The Citizen Lab*, February 2014.

[14] N. Mattise. Syrian electronic army targets reuters again but ad network provided the leak. *ArsTechnica*, June 2014.

[15] 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)*, pages 399–414, 2015.

[16] S. E. McGregor, F. Roesner, and K. Caine. Individual versus organizational computer security and privacy concerns in journalism. *Proceedings on Privacy Enhancing Technologies*, 4:1–18, 2016.

[17] N. Perlroth. Hackers in china attacked the times for last 4 months. *NY Times, Jan*, 30, 2013.

[18] N. Perlroth. Washington post joins list of news media hacked by the chinese. *The New York Times*, 1, 2013.

[19] A. Press. Hackers compromise ap twitter account. `http://bigstory.ap.org/article/hackers-compromise-ap-twitter-account`, April 2013.

[20] I. Raicu. Young adults take more security measures for their online privacy than their elders. `http://www.recode.net/2016/11/2/13390458/young-millennials-oversharing-security-digital-online-p` 2016.

[21] C. Savage. Court rejects appeal bid by writer in leak case. *The New York Times, Oct*, 2013.

[22] S. Sheng, M. Holbrook, P. Kumaraguru, L. F. Cranor, and J. Downs. Who falls for phish?: a demographic analysis of phishing susceptibility and effectiveness of interventions. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 373–382. ACM, 2010.

[23] J. L. Sierra. Digital and mobile security for mexican journalists and bloggers. *Freedom House and the International Center for Journalists*, page I4, 2013.

[24] J. Wagstaff. Journalists, media under attack from hackers: Google researchers, March 2014.