A First Look at the Security and Privacy Perceptions of Sources Who Discussed Sensitive Topics with Journalists

Mahdi Nasrullah
Al-Ameen
malamee@clemson.edu

Byron Lowens
blowens@g.clemson.edu

Susan E. Mcgregor
sem2196@columbia.edu

Kelly Caine
caine@clemson.edu

Introduction. A recent study found that journalists considered the news stories related to the following topics to be *sensitive*: personal information not to be mentioned, vulnerable population, off the record by government officials, and leaked or stolen documents [1]. In this work, we investigated the security and privacy perceptions of sources who discussed sensitive topics with journalists, in terms of their awareness of digital surveillance and relevant privacy issues.

Results and Discussion. We conducted an online survey with 621-U.S.-based participants (580 were usable) through Amazon Mechanical Turk (MTurk). In our survey, 76 participants (half are female and two-thirds of them were between the ages of 25-44) 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 analysis, and noted them as *sources* in this paper.

Twelve of the 76 sources reported using secure communication tools. We identified email and telephone as two of the top three most common medium for journalist-source communication, used by 80% and 70% of sources, respectively. However, a small fraction of sources used them in a secure way: 12% and 5% of sources, respectively, reported using encrypted email and encrypted telephone Our analysis shed light on the possible reasons behind low adoption of secure communication technologies, as noted below.

Misconception about Distant Harm. About one-third (30%) of sources reported that they had already done enough to protect the privacy of their personal information online. However, only four of them reported using secure tools during their communication with journalists. It is possible that users might think it to be unlikely of being a victim of digital attacks, and thus, their perceived level of security threat remains low. To note, people possess a tendency to care less about "distant" harms [2].

Gap between Security Perception and Practices. We identified a gap between security perception and practices of sources. More than two-thirds (71%) of sources noted that people should have the ability to use the Internet completely anonymously for certain kinds of online activities. However, a very few of them reported using anonymous communication tools: four of them used SecureDrop, and two of them used both TOR and SecureDrop during their interaction with journalists. The lack of confidence in finding security tools could be one reason behind this result: two-fifths (41%) of sources reported that it would be "somewhat difficult" or "very difficult" to find secure communication tools and strategies to be more private while using digital devices.

Gap between Security Awareness and Practices. We identified a gap between security awareness and practices of sources: Among that 53% of sources who reported to have heard "a lot" about government surveillance, only 5 (13%) of them used secure communication tools. We also found, around 45% of that sources who had heard "a lot" about government surveillance, reported to be "not at all concerned" about this issue. Thus, for many sources, their awareness of government surveillance might not have translated into concern, and in turn, did not motivate them to adopt secure communication tools. The reduced sense of responsibility for negative outcomes could be a lead factor behind such mental model of users [2].

Demographics and Education. Sources who were above 44 years old (one-fourth of 76 sources), did not use secure tools during their interaction with journalists. Thus, future research should identify the measures to make older users more conscious of using secure communication tools. With 96% of sources having at least some college degree, the low adoption rate of secure communication technologies indicate a gap between general and security education. So, including security education in colleges would benefit those who may discuss sensitive issues with journalists.

Conclusion. One potential solution to improve security and privacy in journalism is to design effective security training modules, where the journalists and information security specialists should work together to achieve this goal.

Acknowledgement. This work is supported in part by NSF Awards CNS-1513875 and CNS-1513663.

References.

[1] S. E. McGregor, P. Charters, T. Holliday, and F. Roesner. Investigating the computer security practices and needs of journalists. In 24th USENIX Security Symposium. 2015.

[2] 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].