Volume 6 Number 7 September 2018

DIGITAL JOURNALISM

Routledge

Digital Journalism

Routledge
Taylor & Francis Group

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/rdij20

Securing Whistleblowing in the Digital Age: SecureDrop and the Changing Journalistic Practices for Source Protection

Philip Di Salvo

To cite this article: Philip Di Salvo (2021): Securing Whistleblowing in the Digital Age: SecureDrop and the Changing Journalistic Practices for Source Protection, Digital Journalism, DOI: 10.1080/21670811.2021.1889384

To link to this article: https://doi.org/10.1080/21670811.2021.1889384

Published online: 17 Mar 2021.

DIGITAL JOURNALISM
https://doi.org/10.1080/21670811.2021.1889384

ORIGINAL ARTICLE

OPEN ACCESS

Securing Whistleblowing in the Digital Age: SecureDrop and the Changing Journalistic Practices for Source Protection

Philip Di Salvo

Institute of Media and Journalism (IMeG), Università della Svizzera italiana (USI), Lugano, Switzerland

ABSTRACT

Information security tools have gained prominence and importance in the journalism field and are now being adopted more frequently by newsrooms and investigative journalists. SecureDrop, an open-source software for operating whistleblowing platforms, is now a common component of the toolboxes of journalists willing to work with stronger levels of security, especially in regard to source protection. By means of a content analysis of publicly available documents and semi-structured interviews with journalists using the software, this article looks at news organizations' uses of SecureDrop, journalists' perceptions of the software's strengths and limitations, and the accountability practices adopted by news organizations in regard to their use of SecureDrop. Overall, this article contributes to the understanding of how SecureDrop and information security in general are entering the journalistic field and becoming accepted journalistic practices.

KEYWORDS

Journalism; information security; SecureDrop; encryption; whistleblowing; source protection; leaks; hacking

Introduction: Securing Journalism on the Internet

Starting in 2013, when leaks about the US National Security Agency's (NSA's) surveillance capabilities started making the news thanks to Edward Snowden's whistleblowing, more and more news organizations have adopted encryption and information security strategies (Shelton 2016). In the context of ubiquitous surveillance and digitalization, software such as Pretty Good Privacy (PGP), the Tor Browser, Signal, and SecureDrop have come to play a crucial part in how journalists effectively protect their work and sources online (Posetti 2017). Research about the adoption of information security tools and practices is a nascent but expanding area of research in the context of journalism studies, especially given the clear role of encryption-based software as protective tools for press freedom (Tsui 2019). So far, studies in this field have focussed on journalists' attitudes towards information security in various countries, such as France, the US, and Hong Kong (McGregor et al. 2015; Pew Research Center

CONTACT Philip Di Salvo philip.di.salvo@usi.ch

2015; Tsui and Lee 2019). Moreover, scholars have instead looked at the organizational or individual patterns driving the adoption of information security in newsrooms (McGregor et al. 2016) or on the current limitations and obstacles impacting the adoption of these practices in the US (Henrichsen 2020). Information security tools in particular have emerged in the literature, dealing with source protection on the Internet (Dreyfus et al. 2013; Bosua et al. 2014). Digital whistleblowing platforms, for instance, are a visible example of how encryption offers effective solutions to journalists who want to cooperate with whistleblowers in order to get tips and leaks and start investigations using digital tools. Whistleblowing platforms are online tools that whistleblowers can approach to submit documents to recipient journalists, using safer and anonymizing technologies based on strong encryption. By offering its online submission system in 2006, WikiLeaks pioneered this technological approach, but now many other organizations are making this practice their own, decidedly, with the help of two distinct yet similar pieces of software: GlobaLeaks and SecureDrop, which are now standardized and used internationally by newsrooms of various kinds (Di Salvo 2020).

SecureDrop, specifically, has become a widely accepted solution among English-speaking newsrooms on both sides of the Atlantic, including mainstream and prominent outlets, such as *The New York Times*, *The Guardian*, *Financial Times*, and the Associated Press. SecureDrop is serving as an important infrastructure for crucial and sensitive journalistic practices and activities, such as the handling of whistleblowers' submissions or leaks, and a crucial tool for the protection of sources on the Internet. This article aims to understand how journalists and newsrooms who adopted SecureDrop conceptualize the use of the software, what motivated its adoption, and how it has impacted the routines and practices of their news work, both in terms of sourcing and accountability. Overall, the article looks at the uses of SecureDrop from a double perspective: the public description of the software on news outlets' websites and journalists' views and ideas emerging from interviews. Overall, the article aims to answer these two research questions:

> *RQ1: What elements and features of SecureDrop are newsrooms publicly describing to their readers and potential sources about their use of the software?*

> *RQ2: How is SecureDrop included in news work and how has it impacted journalists' routines?*

SecureDrop: An Infrastructure for Online Whistleblowing

SecureDrop is one of the most adopted open-source software programs, enabling the creation and launch of online whistleblowing platforms. SecureDrop gives its users the ability to create a communication tool that whistleblowers can use to communicate with recipient journalists in a strongly encrypted manner. In the words of journalist Julia Angwin, SecureDrop works as:

> "an encrypted dropbox that newsrooms can install to allow sources to send documents in an encrypted and anonymous fashion. Sources must download Tor and follow a few simple instructions to send documents through SecureDrop." (2017, 128)

Since SecureDrop operates over the Tor network, whistleblowers have to approach SecureDrop-based platforms with the Tor Browser, which enables access to domains and servers on the Tor network. Originally named DeadDrop, the project is now operated by the US NGO, Freedom of the Press Foundation,[1] which still manages and funds the development of SecureDrop and makes it available via an open-source licence (Berret 2016). At the time of writing, SecureDrop is used by over 35 media organizations, mostly in the US and Western Europe: among the adopters are legacy outlets such as *The Guardian*, *The New York Times*, *The Washington Post,* and digital first, such as *The Intercept*, *Vice, BuzzFeed*, and *The Verge*. SecureDrop provides newsrooms with a complete framework and infrastructure for dealing with whistleblowing over the Internet and with a tested encryption system that has proven to be fundamental in performing source protection in a time of pervasive Internet surveillance (Simon 2015, 112–124; Angwin 2017). SecureDrop is not the only whistleblowing software available to journalists and media organizations, but compared to its European homolog, GlobaLeaks,[2] SecureDrop has a wider and more homogeneous adoption rate among mainstream news outlets (Berret 2016), while GlobaLeaks serves different communities with often stronger and explicit activist traits.

"Boundary Work" in Journalism: The Information Security Way

Information security and encryption software may seem alien to what journalism traditionally intended; for example, research results show a general lack of depth in news reporting about encryption and related issues (Thorsen 2017; Vlavo 2015). Moreover, on a more practical note, journalists have dealt with online secure communications minimally and have invested little resources into their digital hygiene and adoption of safer communication strategies (Pew Research Center 2015). Contrarily, the use of strong encryption-based software is common among privacy-savvy activists, hacktivists, and hackers who base their communication and political strategies on the use of these technologies (Milan and van der Velden 2016). Certainly, encryption-based technologies had some encounters with journalism thanks to the influence and push of various "pioneer journalists" and "pioneer communities" (Hepp and Loosen 2019) that, in the late 1990s and early 2000s explored the potentials of such technologies for reporting purposes. The work of Duncan Campbell, a founding member of the International Consortium of Investigative Journalists (ICIJ), a computer forensic expert, and one of the first reporters to investigate the role of state surveillance in societies, has to be considered as a milestone in this field (Campbell 2015; Leigh 2019, 86–87, 127–130). Later, in the UK, the work of the Centre for Investigative Journalism (CIJ) and its founder, Gavin MacFadyen, led the way to a closer relationship between journalism, whistleblowing, and information security, simultaneously providing a fertile milieu for the collaboration with WikiLeaks and, overall, the practice of leaks-led and data-driven journalism empowered by digital technologies (Hewett 2017). Signs of the presence of hacking, coding, and computer programming traits in journalism can also be traced back to the origins of data journalism and, notably, the pioneering examples of computer-assisted reporting that evolved into today's data-driven reporting (Coddington 2015). Whereas, historically, interest in coding, hacking, and computing was a sign of developments within the field of journalism, the emergence of information security as a journalistic practice has also been the outcome of exchanges between journalists and other external players. Pierre Bourdieu's "Field Theory" (Bourdieu 1996) and Thomas F. Gieryn's notion of "Boundary-work" (Gieryn 1983) both offer insights into these changing journalistic practices and how encryption-based technologies are entering the journalistic field to become common practices among reporters (Russell 2016, 161; Hartley and Ellersgaard 2020). These theoretical frameworks are particularly fruitful in analysing the adoption of newer journalistic practices in the digital context, where the boundaries of journalism are even more visibly in a constant process of negotiation; also, thanks to "liminal" actors that may function as drivers of innovation (Belair-Gagnon, Holton, and Westlund 2019). For instance, the aforementioned data journalism has shown some of the most evident instances of nontraditionally intended practices becoming routinized in reporting, thanks to its combination of data analysis, computing, and information design (Splendore 2017, 41–43). Similarly, activist elements have been increasingly included in the journalism field at the levels of networks, tools, practices, and power (Russell 2016, 68–108). Seen again from Pierre Bourdieu's perspective, the entrance of elements absorbed from outside into journalistic fields is the result of the journalistic field "talking to" other social spaces and contexts (Bourdieu 2005, 31). This more open attitude of the journalistic fields occurs more visibly where the disputes over the fields' boundaries are livelier (Splendore 2017, 21–22) or, to put it Scott Eldridge's terms, in the "periphery" of the journalistic field (2017), where "boundaries between media and non-media fields become highly porous" (Chadwick 2013, 19). Hackers, in parallel with a growing politicization of their own activities (Coleman 2017), have also progressively moved closer to journalism, generating some "boundary-work" (Gieryn 1983) over the attribution of journalistic traits to practices and tools coming from hacking. Recently, journalistic studies have looked at the relationships between hackers and journalists from different perspectives: First, Lewis and Usher, for instance, have looked at this phenomenon using Galison's "trading zones" concept (1997) in different contexts, such as open-source culture (2013), the relationships between journalists and programmers (2016), the "Hacks/Hackers" conferences series, and networks (2014), the growing instances of "interactive journalism" being produced by reporters with strong backgrounds in coding (Usher 2016). The space between information security and journalism is another of these possible "trading zones" (Galison 1997), where journalists absorb and adopt technologies and practice with a clear hacker identity that still respond to journalists' demands and needs, e.g. source protection. Information security tools such as SecureDrop are based on technological standards and practices that have generated and found their familiarity in the hacking community[3] and were created by coders or hackers whose affiliation is not necessarily connected with the journalistic field. Recently, information security has found a place in the journalistic field mostly due to the push by organizations and advocacy groups operating in the field of information security or civic technology, which have offered their collaboration to journalists and news organizations as a response to a growing quest for secure communication, especially from "pioneers" in the journalistic field acting as "intermediaries"[4] between journalism and what is past its boundaries (Hepp and Loosen 2019). As Adrienne Russell writes regarding Tor, for instance:

> "to make these tools more accessible to those outside the tech community, several guides and packages have been created through collaboration among NGOs, advocacy groups, and technology developers." (2016, 94–95)

Moreover, encryption software such as SecureDrop are strongly marked by concepts such as "cryptofreedom" (Coleman and Golub 2008) and "digital resistance" (Ziccardi 2012, 27–30), two representative cultural signifiers of hacking culture: on the one hand, they are used and created by hackers as tools for achieving freedom and empowerment through the development of encryption; on the other hand, they are tools of digital resistance against state and corporate surveillance and various other forms of privacy violations. Whereas these are common stances and ethical premises of hacker culture (Steinmetz and Gerber 2015), they made their mainstream entrance into the journalistic field mostly in the wake of Snowden's surveillance revelations, as is visible by the growing adoption of whistleblowing software, even by prominent international news outlets (Di Salvo 2020, 131–134). Adopting once more Pierre Bourdieu's terms, new players entering the journalistic field (such as hackers) "introduce new elements into the field, enrich the field's capital, and force it to reposition itself *vis-à-vis* [in] other subfields, fields, and the field of power" (Siapera and Spyridou 2012, 82). Thus, the entrance of information security tools into the journalistic field is a sign of contemporary journalism's culture becoming more porous and keen to absorb elements coming from outside, particularly, on the terrain of finding technological solutions that are not necessarily available or producible without joining forces with non-journalistic actors.

Methodology and Sampling

The aim of this article is to look at how newsrooms and journalists conceptualize a) their use of SecureDrop, b) what they identify as the strongest functions of the software, long with c) how they problematize the use of such a critical tool, and d) how they maintain accountability regarding the use of SecureDrop. To structure this analysis, the article is based on a double methodology: 1) a content analysis of publicly available documents and texts on newspapers' websites and 2) semi-structured interviews with investigative reporters using SecureDrop. In order to answer RQ1, for each news outlets, one web page addressing or hosting SecureDrop platforms was analysed ($n = 22$) to understand how news outlets publicly communicate (to their audiences and potential sources) their use of SecureDrop. These pages are usually landing pages where news outlets offer a series of information about how to securely contact the newsrooms and list a series of tools and software, including SecureDrop.[5] Sampled news outlets were selected among the adopters listed on the official SecureDrop project website.[6] Among these, only journalism organizations (newswires, newspapers, both legacy and online only, radio, and TV broadcasters) operating in the English language (the core of the SecureDrop userbase) were considered. Consequently, advocacy, activist, or watchdog organizations were excluded from the sample, together with non-English speaking outlets, to reflect the author's language capacity.

In total, 22 news organizations based in the U.S., U.K., Canada, and Australia were included in the sample. These are: ABC News (Australia), Associated Press (AP), *Bloomberg News*, *BuzzFeed News*, *The Daily Beast*, *USA Today*, CBC News (Canada), *Financial Times*, *Forbes*, Gizmodo Media, *Huffington Post*, *The New York Times*, *The New Internationalist*, *ProPublica*, *The Mail & Globe*, NBC News (USA), *The Guardian*, *The*

Table 1. Four "motivation" arguments for adopting SecureDrop.

Greater security for communication	Associated Press; CBC; Financial Times; Forbes; Globe and Mail; Gizmodo Media; Guardian; New Internationalist; ProPublica; Verge; Vice; Washington Post
Protection of anonymity of the source	ABC News; Bloomberg News; BuzzFeed News; CBC; Gizmodo Media; HuffPost; Globe and Mail; Intercept; Guardian; The Mark-up; New Internationalist; Stuff; Vice
Obfuscation strategies	ABC News; Associated Press; Financial Times; Forbes; HuffPost; Globe and Mail; Gizmodo Media; Guardian; Intercept; The Mark-up; New Internationalist; New York Times; ProPublica; USA Today; Verge; Vice; Washington Post
Turning point	Associated Press; Guardian; USA Today; Washington Post; Vice

Intercept, *The Mark-up*, *The Verge*, *Vice*, and *The Washington Post*.[7] The samples of texts were analysed through a qualitative content analysis (Frey, Botan, and Kreps 1999, 236–239), with the aim of identifying recurring concepts expressed by news outlets. News outlets' motivations and opinions were manually coded and grouped together in categories to consolidate reasoning patterns and similarities. Identified concepts were thus coded inductively and without relying on previously established categories in order to "allow research findings to emerge from the frequent, dominant, or significant themes inherent in raw data, without the restraints imposed by structured methodologies" (Thomas 2006). For the second layer of analysis and to answer RQ2, the author conducted six semi-structured interviews with journalists and reporters working for CBC News, *The Guardian*, *The Huffington Post*, *USA Today*, and *VICE* or by talking in their personal capacity.[8] Interviewees were selected according to their proximity to SecureDrop or by their experience with information security, expressed by different indicators. Journalists were searched for on Twitter; affiliation with the news outlet and the presence of indications for secure communication on their Twitter profiles were considered a sign of proximity to the topic of this article, together with the presence of a work title suggesting closeness to information security or cybersecurity or a senior position in an investigative unit. Interviews were arranged via email and conducted in the first half of 2020 over the phone or VoIP software and lasted about 30 min.[9]

Results: Motivation and Risk Arguments for Adopting SecureDrop

The content analysis of news outlets' public reflections about the adoption of SecureDrop has resulted in the identification of some "motivation" and "risk" arguments that were publicly discussed online by the analysed news outlets while presenting SecureDrop to their audiences and potential sources. In the first group, news outlets' explanations for their reasons for initially using the software emerged, while in the latter, some potential limitations and potential unresolved risks involving the use of the software are expressed. An overview of the results about the motivation arguments is visible and summarized in Table 1, since news outlets tend to use very similar language to express the same concepts.

"Motivation" Arguments

For the adoption of SecureDrop, news outlets publicly offered four different "motivation" arguments: a) the possibility to offer stronger security while communicating with their sources/whistleblowers; b) the opportunity to grant anonymity to sources/whistleblowers; c) the affordances of the "obfuscation"[10] features offered by the software and d) the role of Snowden's revelations as a moment of awareness for the adoption of encryption tools. All outlets have expressed at least two of these "motivation" arguments, as shown in Table 1. When it comes to the need for greater security, three SecureDrop features were generally quoted in this regard: a) the strength of the SecureDrop code itself, b) the reliability and trustworthiness of the news outlets running it, and c) the stronger security safeguards of SecureDrop compared with commercial, online means of communication. Among other SecureDrop's safeguards, which news outlets publicly underline, is the whistleblowers' opportunity to stay anonymous while submitting documents to the recipient news organizations, using the software. Some sampled news outlets mention this point explicitly while describing their work with SecureDrop, implying anonymity as a core value granted to their sources. Moreover, thanks to its technical reliance on the Tor Network, SecureDrop also offers more confidentiality options due to its capability of "obfuscating" communications over the platform, for instance, by hiding metadata.[11] News organizations are keen to stress how SecureDrop is able to encrypt and mask Internet traffic for those approaching a whistleblowing platform operated with the software. Finally, some news organizations also provide more context to their decisions for running SecureDrop in dealing with whistleblowers, discussing which events and circumstances inspired the decision to launch their whistleblowing platform. For these outlets included in the sample, especially for those based in the US or those directly connected with the publication of those leaks, the Snowden case and its aftermath have been indicated as the turning point events inspiring the adoption of safer, encrypted communication tools.

"Risk" Arguments

Sampled news outlets also publicly expressed some concerns about potential risks involved with using SecureDrop to deal with whistleblowers. In this sense, two different "risk" arguments were identified: a) the impossibility of having 100% security from the technology and b) the context of the physical dimension of information security and its technical infrastructure. When it comes to the first point, it is important to mention that the lack of a 100% secure software is a shared opinion among security experts and hackers, including those responsible for SecureDrop, who clearly state on their website that:

> "No, and any organization or product that promises 100% security is not telling the truth. The goal of SecureDrop is to create a significantly more secure environment for sources to share information than exists through normal digital channels, but there are always risks. That said, each release of SecureDrop with major architectural changes goes through a security audit by a reputable third-party security firm."[12]

Thus, some news outlets using SecureDrop also discuss the "100% security" issue by way of recurring and explicit wording choices, reminding their audiences and potential sources that despite the safeguards and solidity of SecureDrop, no sense of total security can be granted. Some news outlets, alternatively, point to the physical dimension of information security, expressing their risk prevention strategies outside

Table 2. Two "risk" arguments for adopting SecureDrop.

No 100% security	ABC News; Daily Beast; USA Today; CBC; Financial Times; Forbes; HuffPost; Globe and Mail; Guardian; The Mark-up; New Internationalist; New York Times; Washington Post
Physical dimension of information security	Bloomberg News; Financial Times; Forbes; BuzzFeed News; Daily Beast; Guardian; New York Times; ProPublica; Vice

of the software dimension only and to a more infrastructural one. For instance, news outlets publicly express how the SecureDrop technical infrastructure is run, referring to the location of the servers running it, whose control is in the hands of the news organizations. This is clearly communicated by some of the news outlets as a sign of risk limitation, trustworthiness, oversight, and transparency. Among these, *BuzzFeed News*, *The Daily Beast*, and *The New York Times* underline with very similar wording how the SecureDrop operations are physically controlled by the news organizations and separated from other potentially vulnerable physical infrastructure running other online operations (Table 2).

From the Interviews: SecureDrop in Practice

The semi-structured interviews investigate five thematic areas: a) motivations for using the software; b) SecureDrop's strengths and positive impacts on news work; c) limitations of SecureDrop; d) amount of content and leaks coming through SecureDrop; and e) accountability practices involved in the use of SecureDrop when it comes to mentioning the software in publicly available documents or articles. In regard to the motivations for using SecureDrop, interviewed journalists have generally expressed similar ideas and comments concerning the safety, reliability. and strength of SecureDrop, especially, in light of the risk of Internet surveillance when it comes to communications with sources. For example, *The Guardian* points to SecureDrop being an effective solution in prominent cases, like those that the newspaper published in recent years:

> "if you're a news organization, you need to make yourself available to sources who have information with varying degrees of security caution. [...] Sometimes people just have tips, sometimes they're happy with their identities be disclosed. They're not all Edward Snowden or Chelsea Manning, but some of them are Edward Snowden or Chelsea Manning." (*The Guardian,* interview, 2020)

Others have indicated SecureDrop's effective tool for preventing surveillance:

> "The motivation for using SecureDrop is to allow journalists to communicate in a secure way with sources or whistleblowers. Due to sophisticated and pervasive surveillance methods that governments and other actors can use, it is very difficult for journalists to communicate safely and confidentially with sources. SecureDrop provides a kind of defence against that kind of surveillance." (Journalist, interview 2020)

Some other news outlets have mentioned specific events or circumstances that have pushed them to start using the software. Again, the Snowden case has been mentioned as turning point events in various instances. Indeed, some news outlets opted to use SecureDrop because they had been directly involved in investigating the Snowden leaks, developing a stronger attention to surveillance:

> "I am the sole journalist who brought SecureDrop to the Canadian Broadcasting Corporation (CBC), in part because I became the Canadian journalist who was working directly with Glenn Greenwald on the Canadian portion of the Snowden leak. […] I was actually concerned about state sponsored, either authorized or unauthorized surveillance of journalists communications, whether that's the NSA and the States, Canada's own intelligence service, which isn't supposed to be spying on its own citizens, other members of the Five Eyes or hostile actors, be it criminal organizations or the Russians or the Chinese." (CBC Canada, interview, 2020)

The Huffington Post, instead, mentioned that the election of Donald Trump as President of the United States played a major part in deciding to use a software to accommodate leaks coming from governmental sources and whistleblowers:

> "We started using it in about 2016 and really the motivation for us was that after Trump was elected, there was a lot of people who worked within government or government institutions who wanted to reach out and speak to us and often wanted to do that through secure platforms. So we wanted to make a better [inaudible] for people to reach us, whether they were in government under Trump, or in other organizations. We wanted to create a better option for them to reach us securely." (*Huffington Post*, interview, 2020)

Various aspects of the security offered by the SecureDrop encrypted ecosystem and its capacity to grant anonymity to sources have been also mentioned by all the interviewed news outlets. Anonymity, in particular, was mentioned as a specific, valuable concept when it comes to handling whistleblowers' submissions. In this regard, SecureDrop is often seen as a state-of-the-art tool for applying this security measure to sourcing. In regard to anonymity, SecureDrop has also been indicated as a solution to the "first contact" problem. Contrarily to other encrypted systems of communication, SecureDrop doesn't require people using it to exchange any personal information, contact details, or private data, so whistleblowers can get in touch with journalists without using any other personal identifier. Whistleblowers can submit their documents virtually and disappear. *The Guardia*n, in particular, stressed this point:

> "Other forms of encrypted technology communication all require the source and the journalist to have already been in contact. There are occasions when we have conversations with sources on Signal or PGP email. You always want to have a portal into your newsroom that someone you haven't already been in touch with can use to securely get in touch." *(The Guardian*, interview, 2020)

The capability to grant anonymity from a technical perspective has been indicated as the specific valuable feature of SecureDrop and as a stronger layer of security for both sources and journalists. In this view, not knowing the identity of the source is considered a plus. CBC Canada, similarly, indicates how anonymity can help in protecting the investigation, while assuring the whistleblower:

> "Not knowing who sent it, would frustrate legal authorities, lawsuits, people trying to gain access to our sources because we simply don't know who they are and technologically it builds in this gap between us and the source. It's ultimately for sources protection, but also when these people use SecureDrop and we haven't met them before, we are trying to provide potential sources with an assurance, a greater assurance that even we won't know who they are." (CBC Canada, interview, 2020)

Some news organizations have also mentioned the problem with spamming incoming content, indicating SecureDrop as a solution to receiving unrequested and spamming emails, a common scenario when email addresses are available freely on a website:

> "It was hard to maintain one organizational email that was encrypted in a way that was also efficient and it kept getting too much spam. With SecureDrop, because it is a little bit tougher to use, people have to really want to send you something. We wanted something that was like both secure and also had a little bit of a bar for people to actually want to reach us. And so it wouldn't get swamped with weird spam." (*Huffington Post*, interview, 2020)

Limitations of SecureDrop mentioned by the interviewed journalists are related to the complexity of the software usage or some of its features. For example, some journalists mentioned the lack of notifications for incoming leaks as a weakness that requires journalists to check the incoming materials and messages regularly, without any prior knowledge of whether anything has been submitted:

> "From a journalist perspective the system is good. It has a few drawbacks: for example, for security reasons, you can't get notifications when a particular person sends a message, and so you have to routinely check it to see if you have received a message. But that is not really a big issue. Generally speaking my experience with SecureDrop has been very positive and I am a big advocate of using it." (Journalist, interview, 2020)

Overall, SecureDrop is indicated as "simple" to use on the journalists' side, while for whistleblowers it has been indicated as functioning on a higher level of complexity. Different interviewed newsrooms have stated, for instance, that the level of security offered by SecureDrop is overly sophisticated for most of the sources who may approach their newsrooms, making it very useful only for a handful of very sensitive sources. Complexity has been indicated also as a potential barrier for non-tech-savvy whistleblowers:

> "I think that they should make it easier for leakers. For journalists it's not that bad and it's just a little bit of an annoying process. You know, once you learn it, you do it. That's fine. But I think it's a little complicated for some leakers as well." (*VICE/Motherboard*, interview, 2020)

For *USA Today*, the inherent complexity doesn't pose a problem to those sources who really feel the need to use SecureDrop, underlining once more how the software is targeted to a limited group of sources. Although this can't be blamed solely on the software design and functionalities, newsrooms have indicated most of the limitations regarding the impact on sourcing and the quantity of actionable leaks obtained via SecureDrop. The number and quality of leaks obtained may depend on various factors: branding and visibility of the news brands, commitment to and history of whistleblowing-led investigations and promotion, and visibility of the software as a solution for sources. Thus, news outlets have indicated various levels of usage of SecureDrop by their sources, but, overall, there seems to be an agreement that even when the platforms attract numerous submissions, only a small percentage is of journalistic value:

> "*USA Today* and our local newsrooms probably have less call to use this than some others like *The New York Times* or *The Washington Post*. We don't t have a particularly robust reporting structure around the intelligence operations of the U.S. government, for example. We have not, to my knowledge, published a story based on information that came to us that way. But we get quite a bit of communication." (*USA Today*, interview, 2020)

At The Guardian, the quality and quantity of incoming submissions vary, although the activity of their SecureDrop appears to be regular:

> "Some mornings we're looking at SecureDrop and there'll be a lot of incoming communications but maybe none of them are of interest to us. Other days there's maybe fewer, but there are two or three things that we will follow up. I want to remain vague, but I'd say there is a regular supply of useful information on a weekly basis that comes to us through SecureDrop." (*The Guardian*, interview, 2020)

In contrast, Vice/Motherboard offers a different picture, with submissions being scarce and relevant ones being rare:

> "We don't get a lot. On average, we get one or two a day at the most. So it's pretty easy to manage. But in terms of useful ones, I think that in the last three or four years could be like one at year that was useful. There have been a few that were promising, but they were not really relevant to us." (*VICE/Motherboard*, interview, 2020)

Also, the variety of documents, leaks, and tips that come through SecureDrop vary; for example, stories and leads don't necessarily refer to high-level or governmental cases, but may still be of interest for a regional beat:

> "We might get one day a tip on a government story in a small city in our eastern provinces, so we would send it off to a journalist who might follow up on that, depending on what the substance is or how sensitive it is, we might help enable communication back to that source or try to say, 'hey, thank you for reaching us through SecureDrop, would you be willing to speak to our reporter directly or through an unencrypted means or a different encrypted means and try to get it over the SecureDrop system to get a direct line of communication?' And so that can be on small things or we get big things and we get newsworthy videos. We also get documents, sensitive documents." (CBC Canada, interview, 2020)

Yet, the quantity of the material that ends up being reported is generally rare, according to the journalists included in the sample for this article. *VICE/Motherboard* shared more details, including some anecdotes, about the differences between actionable content and spam that came through their SecureDrop:

> "I wasn't dreaming that once we set it up the next NSA documents will arrive and we will get a Pulitzer. I didn't think that it was that easy. But I did think that having it would bring more than what it has. […] The people that go to it and use it a lot of them are trolls. The strangest thing, though, to be honest, I will never forget it, was a PDF of an unknown rapper announcing his new mixtape. So it was a PR release in PDF and I was like, ok, I guess he got my attention, but I don't care. So you get a lot of this kind of stuff. Another classic submission is someone claiming to be spied on by the NSA or CIA and in a way that's completely impossible. You know, stuff like they're spying on my brain, they put an implant in my brain 30 years ago." (*VICE/Motherboard*, interview, 2020)

When asked to comment on the overall usage of SecureDrop from their sources, some news outlets underlined again how the security provided by the software could even be overreaching for most sources:

> "We're not overwhelmed. We get a decent amount of things and yes, some some are, you know, viable tips and some are a little bit useless. But I wouldn't say it's overwhelming. What we've found is that most people who need to talk to us can do it through a normal email address. We're not overwhelmed because actually most people don't need that level of security" (*Huffington Post*, interview, 2020)

The last layer of research into the use of SecureDrop by the sampled news outlets referred to the accountability practices connected to the use of the software or other policies in regards of accountability and transparency. Most news outlets declared not to have specific editorial policies in this sense. *The Huffington Post* stated:

> "We absolutely say that we're using it. I don't think that we would ever say in a story that this came through our SecureDrop. We'd probably think that is kind of meaningless to most of our readers. That's something that other journalists would care about. But most readers would be like, what's that? We don't really put that in an article. But it certainly it is clearer on our site and our articles: that's like how you would contact us that way if you wanted to" (*Huffington Post*, interview, 2020)

For others, public references to SecureDrop is done only in those instances where a contribution from a source may be useful and, consequently, be solicited:

> "If we're doing a story that we think someone might want to upload or send us information that is sensitive, we might note in that story that we have secure communication available. I think that's been pretty rare that we've done it. I think we've done a little bit of promotion on the Web site to let people know that we are cognizant of their security concerns and we want to hear from them if they have sensitive information" (*USA Today*, interview, 2020)

For some other outlets, mentioning SecureDrop as the sourcing channel for a story is decided on a case-by-case basis and in accordance with the sources and their specific security needs. VICE/Motherboard discusses a specific case:

> "Three years ago we did that big 'stalkerware' investigation[13] and part of it came from SecureDrop and we did mention it. In that case, we asked the source if it was ok to mention it and they agreed. So I guess that is our policy: is the source ok with it? If not we don't mention it." (*VICE/Motherboard*, interview, 2020)

Moreover, for some news outlets, not mentioning this kind of information is also another layer of source protection. *The Guardian*, notably, prefers to bring awareness to the existence of the platform without explicitly stating in stories that a leak came via SecureDrop:

> "I think there is some sort of security benefit in remaining vague or not specify how information comes to you. There's another side to this which you simply do enough people know the security exist? One of the things I'm planning to do in the months ahead is, is try to improve our proactive use in encouraging people to contact us via SecureDrop. It is important to be calibrated in the way you do that, because it is quite a high barrier for entry" (*The Guardian*, interview, 2020)

Conclusion and Discussion

Results from the news outlets' sample gathered for this article confirm the existence of a growing interest in adopting information security solutions and technologies in the journalistic field, especially, for source protection. Particularly, results provide more evidence about how SecureDrop is progressively becoming an established practice for prominent news outlets in the Anglo-Saxon context. Results of this explorative article are straight-forward: news outlets are expressing similar motivations and needs when it comes to securing their communications and granting confidentiality or anonymity to their sources both publicly and in interviews. This is in line with previously available research on source protection in the digital age, where fears about potential exposure of confidential sources because of governmental surveillance activities were expressed by investigative reporters (Lashmar 2017) and are considered among the most pressing issues for contemporary journalism at large (Posetti 2017; Schultz and Belair-Gagnon 2017; Posetti, Dreyfus, and Colvin 2018). In addition, previous research concerning information security cultures in journalism have shown that, generally, journalists consider source protection as the "chief concern" in regard to security (Crete-Nishihata et al. 2020, 10). SecureDrop has emerged as one of the most helpful tools when it comes to performing these critical journalistic principles and granting anonymity with a stronger level of security. Results also show also how the growing adoption of encryption tools and wider attention to the issue of information security are definitely some of the most visible elements of the so-called "Snowden effect" (Gorman 2017) on journalism. In other words, the overall impact of the case on the practice of journalism, together with the greater availability of other tools, is helping journalists protect their work (Angwin 2017; O'Brien 2015; Thorsen 2019).

Analysed news outlets intelligibly and publicly expressed the risks involved with the use of SecureDrop in journalism, especially on the side of their users and whistle-blowers, in particular. For instance, all sampled news outlets demonstrated both confidence and conscious concern regarding the security of their software. These results show a shared and diffused attention for media accountability, intended as "the expectations of relevance, credibility, and quality of public communication set by society" (Domingo and Heikkilä 2012, 272). In this sense, SecureDrop also works as a trust signifier that news outlets can adopt to reinforce their commitment to investigative, watchdog-oriented journalism and adherence to classic journalistic premises, such as source protection, specifically, in the digital age. Analysed news outlets expressed their views on these security matters with a high level of transparency, together with the communication of risks, which are overall readily stated to their readers and potential sources. Moreover, a general enthusiasm from journalists about SecureDrop is clearly visible: the software is perceived as a reliable if not indispensable tool for security and whistleblowing-solicitation in the digital age. In this sense, no tension emerged in comparison with arguments and published statements on news outlets' websites. Whereas news outlets share common views about the strengths and advantages of the software, most of the limitations noted during the interviews were related to the amount of journalistically relevant content that newsrooms are able to obtain through SecureDrop. This varies according to different elements, but overall, SecureDrop seems to be effective in a limited set of cases and in regard to very sensitive sources and stories. In the words of an interviewed journalist:

> "When Kevin Poulsen launched it, he said that it was a ramp for disabled people. In your restaurant, you want to have a ramp, not because you have people in wheelchairs coming in every day, but because maybe one day someone will come to your restaurant and you want to be able to accommodate that. That, to me, is SecureDrop" (*VICE/Motherboard*, interview, 2020)

Whereas SecureDrop has extensively been indicated as a crucial and reliable tool for the securing of news work, its impact on sourcing shouldn't be overestimated in terms of bringing new major, international whistleblowing cases too easily. As emerged from the interviews, SecureDrop may be working on an excessively high level of security for most sources that may approach news outlets with tips or leaks. This may potentially create a “divide” between tech-savvy and less skilled sources, who may be left exposed to greater risks. Overall, SecureDrop appears to be considered a standard solution that has to be made available “just in case” and as a response to potential high-ranking whistleblowers who really need such a level of security. This result is in line with what has emerged from previous research about US journalists’ attitudes about information security, who usually believe security measures are needed only when they work with government-level sources or very sensitive information (Henrichsen 2020) or with research on journalists’ “mental models” about information security (McGregor and Watkins 2016). Results of this article also confirm the “security by obscurity” mental model, a belief by which high security safeguards, like those offered by SecureDrop, are only perceived as necessary when journalists are involved in work that may “attract the attention of government actors” (McGregor and Watkins 2016, 39). Similarly to Crete-Nishinata et al.’s results (2020), this article also indicates that the beats followed by journalists play a significant part in deciding their personal security approach: the highest standards of information security are usually considered here as a must only in relation to specific investigations, such as those in connection with governmental or intelligence issues. On a broader holistic level, the details about the use of SecureDrop by news outlets are also adding new elements to the understanding of how journalism is undergoing a process of “boundary work” involving hacker technologies and practices. Notably, these results show how this process can be based on “integration” (Chadwick 2013, 15), as what has been discussed shows the progressive acceptance of some classic hacker technology and practices in the journalistic field. The relevance of SecureDrop is visible in how it can help support source protection in the digital age, a core element of the “habitus” around which the journalistic field is organized. Based on the results of this article regarding SecureDrop, some specific technical skills have been introduced in the journalistic field from the hacking world, explicitly, with the purpose of supporting some of the core elements of journalism. Inevitably, this research presents some limitations. Thus, further research should be conducted to overcome some of the shortcomings of this article, particularly, with respect to the sample size and its culture. This article only focussed on a homogeneous sample of English-speaking outlets based in English-speaking countries, with similar democratic standards, strong economies, and journalistic markets. The understanding of how elements of hacking are influencing contemporary journalism definitely needs further analyses and contributions from different journalistic cultures and social contexts.

Notes

1. https://freedom.press/
2. GlobaLeaks is another whistleblowing solcitation software, coded and managed by the Italian NGO Hermes Center for Transparency and Human Digital Rights. The software homepage is available here: https://www.globaleaks.org/

3. The original conceptualization of SecureDrop was made by *Wired* magazine editor Kevin Poulsen. Still, the technical development of the software was pushed forward by the late hacker and activist Aaron Swartz in 2012. Poulsen spoke of Swartz as "a member of a fairly small tribe with the skills to turn ideas into code" describing Swartz' role in the creation of SecureDrop (Berret 2016).
4. The term "intermediaries", as quoted in Hepp and Loosen (2019) is again taken from Pierre Bourdieu (2010)
5. *The Guardian* and the *New York Times* offer two of the most comprehensive of such pages. They are linked here as examples: https://www.nytimes.com/tips and https://www.theguardian.com/help/ng-interactive/2017/mar/17/contact-the-guardian-securely. These pages are available from news outlets' homepages.
6. Available here: https://securedrop.org/directory/
7. The San Francisco Chronicle was not included in the sample because its SecureDrop page is not available outside the US for "legal reasons".
8. This is the case of a journalist with experience with bot *The Intercept* and *Bloomberg News*, speaking in personal terms. This interviewee will be indicated as "Journalist" in the Results section. Other quotes are instead attributed to news outlets.
9. The author contacted at least one journalist for each news organization included in the sample. In some cases it was not possible to establish a point of contact or to plan an interview because of lack of responses. Among the news outlets that was not possible to include in the interview sample, only the *Financial Times* explicitely denied an interview on the basis of not wanting to discuss security measures or source protection matters.
10. "Obfuscation" has been described by Finn Brunton and Helen Nissenbaum as "the production of noise modeled on an existing signal in order to make a collection of data more ambiguous, confusing, harder to exploit, more difficult to act on, and therefore less valuable." (2015, 46)
11. "Obfuscation" has been described by Finn Brunton and Helen Nissenbaum as "the production of noise modeled on an existing signal in order to make a collection of data more ambiguous, confusing, harder to exploit, more difficult to act on, and therefore less valuable" (2015, 46)
12. Available here: https://securedrop.org/faq/about-securedrop/#does-securedrop-promise-100-security
13. Available here (Franceschi-Bicchierai and Cox 2017): https://www.vice.com/en_us/article/53vm7n/inside-stalkerware-surveillance-market-flexispy-retina-x

Acknowledgements

I would like to thank Prof. Oscar Westlund, the *Digital Journalism* editorial team and all the anonymous reviewers for their dedication and fundamental contribution in pushing this article ahead and making it stronger. Also, I'm grateful to all the interviewed journalists who, in one of the most complex time for journalism, allocated some time to answer my questions.

Disclosure Statement

No potential conflict of interest was reported by the author.

References

Angwin, Julia. 2017. "Digital Security for Journalists." In *Journalism after Snowden. The Future of the Free Press in the Surveillance State*, edited by Emily Bell and Taylor Owen, 114–130. New York: Columbia Journalism Review Books.

Belair-Gagnon, Valerie, Avery E. Holton, and Oscar Westlund. 2019. "Space for the Liminal." *Media and Communication* 7 (4): 1–7.

Berret, Charles. 2016. "Guide to SecureDrop." *Tow Center for Digital Journalism*. Accessed September 7, 2020. https://legacy.gitbook.com/book/towcenter/guide-to-securedrop/details.

Bosua, Rachelle, Simon Milton, Suelette Dreyfus, and Reeva Lederman. 2014. "Going Public: Researching External Whistleblowing in a New Media Age." In *International Handbook on Whistleblowing Research*, edited by A. J. Brown, 250–272. Cheltenham: Edward Elgar Publishing.

Bourdieu, Pierre. 1996. *The Rules of Art. Genesis and Structure of the Literary Field*. Redwood City, CA: Stanford University Press.

Bourdieu, Pierre. 2005. "The Political Field, the Social Science Field, and the Journalistic Field." In *Bourdieu and the Journalistic Field*, edited by Rodney Benson and Erik Neveu, 29–48. Cambridge: Polity.

Bourdieu, Pierre. 2010. *Distinction*. New York: Routledge.

Brunton, Finn, and Helen Nissenbaum. 2015. *Obfuscation. A User's Guide for Privacy and Protest*. Cambridge, MA: The MIT Press.

Campbell, Duncan. 2015. "My Life Unmasking British Eavesdroppers." *The Intercept*. Accessed August 3, 2020. https://theintercept.com/2015/08/03/life-unmasking-british-eavesdroppers/.

Chadwick, Andrew. 2013. *The Hybrid Media System: Politics and Power*. Oxford: Oxford University Press.

Coddington, Mark. 2015. "Clarifying Journalism's Quantitative Turn. A Typology for Evaluating Data Journalism, Computational Journalism, and Computer-Assisted Reporting." *Digital Journalism* 3 (3): 331–348.

Coleman, Gabriella. 2017. "From Internet Farming to Weapons of the Geek." *Current Anthropology* 58 (S15): S91–S112.

Coleman, Gabriella, and Alex Golub. 2008. "Hacker Practice: Moral Genres and the Cultural Articulation of Liberalism." *Anthropological Theory* 8 (3): 255–277.

Crete-Nishihata, Masashi, Joshua Oliver, Christopher Parsons, Dawn Walker, Lokman Tsui, and Ronald Deibert. 2020. "The Information Security Cultures of Journalism." *Digital Journalism* 8 (8): 1068–1091. Published online June 25, 2020.

Di Salvo, P. 2020. *Digital Whistleblowing Platforms in Journalism. Encrypting Leaks*. London: Palgrave Macmillan.

Domingo, David, and Heikki Heikkilä. 2012. "Media Accountability Practices in Online News Media." In *Handbook of Global Online Journalism*, edited by Eugenia Siapera and Andreas Veglis, 272–289. Chichester, UK: Wiley-Blackwell.

Dreyfus, Suelette, Reeva Lederman, A. J. Brown, Simon Milton, Marcia P. Miceli, Rachelle Bousa, Andrew Clausen, and Jessie Schanzle. 2013. "Human Sources: The Journalist and the Whistleblower in the Digital Era." In *Journalism Research and Investigation in a Digital World*, edited by Stephen Tanner and Nick Richardson, 48–61. Melbourne: Oxford University Press Australia & New Zealand.

Eldridge, Scott A. 2017. *Online Journalism from the Periphery. Interloper Media and the Journalistic Field*. London: Routledge.

Franceschi-Bicchierai, Lorenzo, and Joseph Cox. 2017. "Inside the 'Stalkerware' Surveillance Market, Where Ordinary People Tap Each Other's Phones." *Motherboard*. Accessed April 18, 2020. https://www.vice.com/en_us/article/53vm7n/inside-stalkerware-surveillance-market-flex-ispy-retina-x.

Frey, Lawrence, Carl Botan, and Gary Kreps. 1999. *Investigating Communication: An Introduction to Research Methods*. Boston, MA: Allyn & Bacon.

Galison, Peter. 1997. *Image & Logic: A Material Culture of Microphysics*. Chicago, IL: The University of Chicago Press.

Gieryn, Thomas F. 1983. "Bounday-Work and the Demarcation of Science from Non-Science: Strains and Interests in Professional Ideology of Scientists." *American Sociological Review* 48 (6): 781–795.

Gorman, Siobhan. 2017. "The Snowden Effect on the NSA and Reporting." In *Journalism after Snowden. The Future of the Free Press in the Surveillance State*, edited by Emily Bell and Taylor Owen, 197–208. New York: Columbia Journalism Review Books.

Hartley, Jannie Møller, and Christoph Houman Ellersgaard. 2020. "Mapping Online Journalism in Transition: Exploring an Analytical Model." *Nordicom Review* 34 (s1): 43–61.

Henrichsen, Jennifer R. 2020. "Breaking through the Ambivalence: Journalistic Responses to Information Security Technologies." *Digital Journalism* 8 (3): 328–346.

Hepp, Andrew, and Wiebke Loosen. 2019. "Pioneer Journalism: Conceptualizing the Role of Pioneer Journalists and Pioneer Communities in the Organizational Re-Figuration of Journalism." *Journalism*: 146488491982927. First published February 19, 2019. https://journals.sagepub.com/doi/full/10.1177/1464884919829277

Hewett, Jonathan. 2017. "Collaborative Learning: From CAR to Data Journalism and Hacks/Hackers." In *Data Journalism: Past, Present and Future*, edited by John Mair, Richard L. Keeble, and Megan Lucero, 5–22. Bury St. Edmunds: Abramis.

Lashmar, Paul. 2017. "No More Sources? The Impact of Snowden's Revelations on Journalists and Their Confidential Sources." *Digital Journalism* 11 (6): 665–688.

Leigh, David. 2019. *Investigative Journalism. A Survival Guide*. London: Palgrave Macmillan.

Lewis, Seth C., and Nikki Usher. 2013. "Open Source and Journalism: Towards New Frameworks for Imagining News Innovation." *Media, Culture & Society* 35 (5): 602–619.

Lewis, Seth C., and Nikki Usher. 2014. "Code, Collaboration, and the Future of Journalism: A Case Study of the Hacks/Hackers Global Network." *Digital Journalism* 2 (3): 383–393.

Lewis, Seth C., and Nikki Usher. 2016. "Trading Zones, Boundary Objects, and the Pursuit of News Innovation: A Case Study of Journalists and Programmers." *Convergence: The International Journal of Research into New Media Technologies* 22 (5): 543–560.

McGregor, Susan E., and Elizabeth Anne Watkins. 2016. "Security by Obscurity: Journalists' Mental Models of Information Security." *International Symposium on Online Journalism (ISOJ)* 6 (1): 33–51.

McGregor, Susan E., Franziska Roesner, and Kelly Kaine. 2016. "Individual versus Organizational Computer Security and Privacy Concerns in Journalism." In *Proceedings on Privacy Enhancing Technologies* 4: 418–435.

McGregor, Susan E., Polina Charters, Tobin Holliday, and Franziska Roesner. 2015. "Investigating the Computer Security Practices and Needs of Journalists." In *Proceedings of the 24th USENIX Security Symposium*, 399–414.

Milan, Stefania, and Lonneke Van der Velden. 2016. "The Alternative Epistemologies of Data Activism." *Digital Culture & Society* 2 (2): 57–74.

O'Brien, J. Kelly. 2015. "Why Encryption Is Crucial for All News Organizations." *Columbia Journalism Review*. Accessed March 31, 2020. https://www.cjr.org/analysis/encryption_for_all_reporters_not_just_natsec_ones.php.

Pew Research Center. 2015. "Impact of Security Concerns on News Reporting." Accessed March 31, 2020. https://www.journalism.org/2015/02/05/impact-of-security-concerns-on-news-reporting/.

Posetti, Julie, Suelette Dreyfus, and Naomi Colvin. 2018. "The Perugia Principles for Journalists Working with Whistleblowers in the Digital Age." Blueprint for Free Speech. Accessed March 31, 2020. https://blueprintforfreespeech.net/wp-content/uploads/2019/01/Blueprint_Perugia_Principles.pdf.

Posetti, Julie. 2017. "Protecting Sources in the Digital Age." United Nations Educational, Scientific and Cultural Organization. Accessed March 31, 2020. http://unesdoc.unesco.org/images/0024/002480/248054E.pdf.

Russell, Adrienne. 2016. *Journalism as Activism. Recoding Media Power*. Cambridge: Polity.

Schultz, David A., and Valerie Belair-Gagnon. 2017. "Rescuing a Reporter's Right to Protect the Confidentiality of Sources." In *Journalism after Snowden. The Future of the Free Press in the Surveillance State*, edited by Emily Bell and Taylor Owen, 97–113. New York: Columbia Journalism Review Books.

Shelton, Martin. 2016. "How 10 News Orgs Adopted PGP Email Encryption (Or Not)." *Medium*. Accessed April 1, 2020. https://medium.com/@mshelton/how-10-news-orgs-adopted-pgp-or-not-cc278531a82b.

Siapera, Eugenia, and Lia-Paschalia Spyridou. 2012. "The Field of Online Journalism: A Bourdieusian Analysis." In *Handbook of Global Online Journalism*, edited by Eugenia Siapera and Andreas Veglis, 77–97. Chichester, UK: Wiley-Blackwell.

Simon, Joel. 2015. *The New Censorship. Inside the Global Battle for Media Freedom*. New York: Columbia University Press.

Splendore, Sergio. 2017. *Giornalismo Ibrido. Come Cambia la Cultura Giornalistica Italiana*. Roma: Carocci.

Steinmetz, Kevin, and Jurg Gerber. 2015. "It Doesn't Have to Be This Way": Hacker Perspectives on Privacy." *Social Justice* 41: 29–51.

Thomas, David R. 2006. "A General Inductive Approach for Analyzing Qualitative Evaluation Data." *American Journal of Evaluation* 27 (2): 237–246.

Thorsen, Einar. 2017. "Cryptic Journalism. News Reporting of Encryption." *Digital Journalism* 5 (3): 299–317.

Thorsen, Einar. 2019. "Surveillance of Journalists/Encryption Issues." In *The International Encyclopedia of Journalism Studies*, edited by Tim P. Vos and Folker Hanusch. Hoboken, NJ: Wiley. https://www.wiley.com/en-us/The+International+Encyclopedia+of+Journalism+Studies+%2C+3+Volume+Setp-9781118841679

Tsui, Lokman, and Francis Lee. 2019. "How Journalists Understand the Threats and Opportunities of New Technologies: A Study of Security Mind-Sets and Its Implications for Press Freedom." *Journalism:* 146488491984941. First published May 19, 2019. https://journals.sagepub.com/doi/pdf/10.1177/1464884919849418.

Tsui, Lokman. 2019. "The Importance of Digital Security to Securing Press Freedom." *Journalism* 20 (1): 80–82.

Usher, Nikki. 2016. *Interactive Journalism: Hackers, Data, and Code*. Urbana: University of Illinois Press.

Vlavo, Fidele. 2015. "Framing Digital Activism: The Spectre of Cyberterrorism." *First Monday* 20 (10): https://firstmonday.org/ojs/index.php/fm/article/view/6139/5001

Ziccardi, Giovanni. 2012. *Resistance, Liberation Technology and Human Rights in the Digital Age*. London: Springer.