Received: 14 October 2021 | Revised: 13 January 2022 | Accepted: 17 January 2022

DOI: 10.1111/soc4.12961

ARTICLE

WILEY

Information security and journalism: Mapping a nascent research field

Philip Di Salvo[1,2]

[1]Department of Media and Communications, The London School of Economics and Political Science, London, UK

[2]Institute of Media and Journalism, Università della Svizzera italiana, Lugano, Switzerland

Correspondence
Philip Di Salvo, Department of Media and Communications, The London School of Economics and Political Science, London, UK.
Email: philip.di.salvo@usi.ch

Funding information
The Swiss National Science Foundation (SNSF), Grant/Award Number: P2TIP1_191492

Open access funding provided by Università della Svizzera italiana

Abstract

Information security (infosec) has become a field of primary interest for journalism, especially in the wake of the 2013 Edward Snowden revelations about the ramifications of Internet mass surveillance. Following the increasing dangers posed by digital threats—and surveillance in particular—to the safety of journalists and their sources, newsrooms and reporters have shown an increased interest in technological solutions for improved protection of their work and sources. In particular, the adoption of strong encryption tools for communication purposes has become an urgent matter for journalists worldwide, becoming a niche of research in journalism studies as well. By reviewing the existing literature in the field, this article examines how journalism studies approach the use of encryption and information security tools for journalistic purposes. Based on research on the major journalism studies journals and other publications, the article offers an overview of the research advancements, highlighting current major trends and research areas.

KEYWORDS
cryptography, encryption, hacking, information security, investigative journalism, journalism, surveillance, whistleblowing

1 | INTRODUCTION

With the growing number of digital attacks and surveillance operations that target journalists, the issue of information security (hereafter, infosec) has become even more crucial for the field, in parallel with other security issues threatening journalism freedom in the physical realm (Carlsson & Pöyhtäri, 2017). The 2013 Snowden revelations have constituted "a historic and urgent wake-up call" regarding concerns about surveillance and overall the use of infosec (Coleman, 2019, p. 568). As Coleman argues (2019), the global magnitude of the Snowden scandal has also contributed to making strong encryption software, such as SecureDrop or Signal, increasingly accessible and common among various communities, including journalists (Berrett, 2017). Before the Snowden revelations, encryption tools were minimally used in the newsrooms, which lacked the needed awareness about digital surveillance (Waters, 2017). Overall, the coverage of encryption-related issues has also increased significantly, following the publication of the Snowden's leaks (Thorsen, 2016). Other scandals have followed Snowden's whistleblowing, pushing up infosec topics to even higher rankings in journalism's agenda. For instance, the Cambridge Analytica case has raised new concerns about data manipulation and weaponization (Hu, 2020), while the 2021 revelations about the international proliferation of the Pegasus[1] spyware has rung another bell about surveillance-related risks for journalists and the dangers posed by intrusive technologies to journalism as a whole (Kirchgaessner et al., 2021). For all these reasons, for journalists, "to practice digital security is to exercise press freedom as a positive liberty" (Tsui, 2019, p. 82). In particular, the journalists' reliance on encryption tools has to be contextualized in light of the broader dangers that surveillance poses to safety and freedom in the field.

2 | JOURNALISM IN THE SURVEILLANCE SOCIETY AND ENCRYPTION AS A RESPONSE

The ubiquitous diffusion of computers, digital technologies at large, and the rise of the information society are all connected with an increase in surveillance. For Burnham, computers mass-produce "transactional information," documenting anyone's personal details by storing them (Burnham, 1990, pp. 94–106). For David Lyon, the so-called information society is a *de facto* surveillance society (Lyon, 2001). This is due to the mass availability of personal data and information and the explosion of tracking and monitoring capabilities, which are at the core of an enormous number of new surveillance scenarios and practices, operated by both private entities and state actors. In this context, a variety of digital threats capable of jeopardizing journalists' safety and freedom has also emerged as a side effect, ranging from mass surveillance to sophisticated, targeted attacks, such as phishing or other hacking attempts (Henrichsen et al., 2015). In 2013, the Snowden revelations exposed how the US National Security Agency and other federal agencies had the capabilities to conduct various kinds of surveillance operations—ranging from bulk interception of data in transit to targeted surveillance—and the different legal instruments available to conduct surveillance that violates journalists' freedom, even without a warrant (Boghosian, 2013, pp. 173–188; Henrichsen & Bloch-Wehba, 2017). These activities (which are definitely not undertaken by the US only), especially due to their unaccountable nature and secretive use, have raised concerns among human rights organizations for their potential chilling effects on journalists (Human Rights Watch & American Civil Liberties Union, 2014). Regarding targeted surveillance, there is growing evidence of how spyware and other malicious hacking tools are being used to target civil society organizations and journalists. The University of Toronto's Citizen Lab[2] has extensively researched this issue, documenting the use of spyware against journalists in different countries, including Mexico (Scott-Railton et al., 2018), Saudi Arabia, and the United Arab Emirates (Marczak et al., 2020), among others. Already in 2018, the Citizen Lab gathered evidence of the use of the Pegasus spyware in 45 countries, including seven European nations (Marczak et al., 2018). Among other forms of digital surveillance, spyware is definitely the most pervasive one, and it can compromise the security, freedom, and independence of journalists to the core (Woodhams, 2021).

Against these threats, infosec and cryptography are traditionally included among successful anti-surveillance practices (Leistert, 2012). Per se, infosec lacks a shared definition among computer scientists, as most of the definitions available in the literature tend to indicate what infosec *does*, rather than what it *is* (Anderson, 2003). Among the other available definitions, Neumann's is probably the one that fits best in relation to the application of infosec to the practice of journalism. In his view, infosec "implies freedom from danger, or, more specifically, freedom from undesirable events such as malicious and accidental misuse. Security is also a measure of how well a system resists penetrations by outsiders and misuse by insiders" (Neumann, 1995, as cited in; Anderson, 2003, p. 310). Traditionally, infosec involves at least three elements—*Confidentiality*, *Integrity*, and *Availability* (usually known as CIA), respectively the prevention of unauthorized reading of information, the detection of unauthorized changes to data, and the safeguarding of reduced access to information—performed through the use of software and security protocols and cryptography (Stamp, 2011, pp. 2–4). The three CIA elements can be adapted to the practice of journalism, as they can be set up in relation to some risk scenarios common in newsmaking, such as source protection (Confidentiality), freedom from external interferences (Integrity), and protection from attacks and limitations to speech (Availability). In this regard, infosec is closely related to the practice of journalism in a digital context and to the threats and dangers arising from digitalization, including surveillance, hacking, and potential monitoring via spyware.

Cryptography and encryption—which involve the development and use of secret codes to mask the content of communication—comprise a branch of mathematics that transforms data to keep messages secret and safe from a series of risks, including unauthorized access and interception (Peltier et al., 2005, p. 155). Infosec tools, such as privacy-enhancing technologies, "promise to enable individuals to take control over how their data is being collected" (Seničar et al., 2003, p. 151). Relying on cryptography protocols, these technologies provide solutions to surveillance issues related to the use of digital technologies or digital channels to journalists as well. For instance, they can provide anonymity to email systems, protecting identities when Internet services are being used or shielding the contents of Internet conversations (Goldberg, 2008, pp. 5–13). Overall, encryption is "the method for protecting digital information, whether it's in transit (moving across the Internet) or at rest (saved on your local hard drive or on a cloud server somewhere)" (McGregor, 2021, p. 57). Although encryption is now embedded in most Internet services and network technologies as a *de facto* security feature and infrastructure, its origins have subversive traits, especially in how activists used it in the 1990s as an instrument with radical potentials. Thus, cryptography possesses eminently political traits (Monsees, 2020, p. 58). For instance, the early 1990s Cypherpunk movement had its politics gravitating mostly toward the use of cryptography and infosec as instruments to frustrate government surveillance (Jarvis, 2021). Overall, the hacker culture, along its heterogeneous historical evolution, has always regarded cryptography and infosec as statutory elements, mixed with an anti-authoritarian stance and a privacy-oriented attitude expressed as a clear anti-surveillance sentiment (Kubitschko, 2015; Taylor, 1999, p. 62). Moreover, hacktivism—or "activism gone electronic" (Jordan & Taylor, 2004, p. 1)—is based on the use of digital technologies for either direct action or for "defending and extending the peculiar powers cyberspace creates" (Jordan & Taylor, 2004, p. 116). Various hacktivist groups have pursued these goals by "radicalizing hacking's original obsession with information freedom and access by creating tools that ensure cyberspace remains a place where information is freely and securely available" (Jordan & Taylor, 2004, p. 4). Hacktivists who develop some of the software that are discussed in this article have also been defined as "radical techies" (Milan, 2013, pp. 45–48), a definition that stresses how these hacktivist organizations "provide alternative communication channels on the Internet to activists and citizens" (p. 12), with a clear focus on encryption systems and open-source software.

The expansion of the surveillance apparatus in the hands of the government and the blatant use of surveillance technologies against journalists and their sources have driven journalism to look at cryptography and infosec and to start adopting similar solutions (Di Salvo, 2021b). In hacker-journalist Micah Lee's words, "it's really difficult to do (journalism via digital tools) without leaving lots of traces everywhere" (Lee & Heinrichs, 2019, p. 811). The whistleblowing organization WikiLeaks, whose leaks-solicitation dropbox is based on various cryptography protocols, has definitely been the most explicit and successful in accomplishing this goal (Brevini, 2017; Chadwick, 2013, pp. 103–129; Heemsbergen, 2013). Since 2006, Julian Assange's organization has been able to obtain and publish, mostly in

partnership with international media, some sensitive, impactful, and controversial releases, starting an era where leaks have deeply affected the broader media ecology (Hintz, 2019). Other encryption solutions (for whistleblowing and beyond) are now becoming common in numerous newsrooms internationally (Di Salvo, 2020, pp. 103–136; 2021; Higgins, 2020).

In light of this increased centrality of encryption for journalists, it is worth investigating how the field of journalism studies has addressed these phenomena with dedicated research. This article aims to offer an initial (and obviously not conclusive) mapping of how scholars in journalism studies have analyzed the spread of infosec among journalists by highlighting research trends in the existing literature. This research was conducted following a two-step methodology. First, the top 100 English-language journals included in the Scimago Journal & Country Ranking for "Communication" were considered. The potentially relevant articles were retrieved in September 2021 by means of online searches on the journals' databases using the keyword "encryption." Of all the results obtained from the databases, only those articles explicitly focusing on issues related to the use of infosec tools for journalistic purposes were included in the sample. In the second step of the research, the sample was enriched by including further articles, book chapters, and volumes quoted in the literature in order to better reflect scholarly works available beyond the Scimago ranking. The articles included as a result of this second analysis were chosen according to the information presented in their abstracts in order to establish whether they explicitly concern infosec and journalism. The books and the book chapters included in the analysis were chosen on the basis of the author's previous research in the area. Later, a thematic analysis (Braun & Clarke, 2006) of the sample was conducted to identify relevant research areas and trends. Finally, the articles were coded the first time to let the research topics emerge clearly and were later combined within larger groups, which became the two major themes discussed in the analysis.

3 | TWO EMERGENT AREAS OF RESEARCH

This literature review shows the emergence of two different research themes. Overall, the articles can be classified in the following research areas/topics: (a) the use of infosec tools and practices in journalistic contexts and (b) motivations, rationales, and organizational issues related to infosec in a journalistic context. The articles included in the first group mostly address the analysis of specific infosec practices or the use of specific tools in various journalistic contexts or in response to various digital threats to journalistic practices. The articles comprising the second group relate to research on journalists' views and ideas about infosec or organizational matters involved in the use of infosec in newsrooms. Overall, in journalism studies, the scholars' interest in infosec and journalism appears to be focused on two different paths: an *instrumental* one, based on the analysis of how journalists use and adopt infosec, and a more *cultural* one, dealing with why and on which basis infosec finds a place in journalism and due to which drivers and actors. However, these two research areas should not be intended as standards, and their boundaries are not strict or perfectly identifiable all the time. In fact, a significant number of the articles analyzed in this review present elements of both areas, sometimes with an overlapping analytical lens. For clarity, their inclusion in one of the areas has been decided on the basis of the prominence of either an instrumental or a cultural perspective on infosec in journalism. The articles analyzed in this literature review involve different research traditions, backgrounds and approaches, including but not limited to media and journalism studies, surveillance studies and organizational studies. Overall, most of research conducted in this area appears to be qualitative in nature with a prevalence of interviews as the most frequently adopted methodology of inquiry.

3.1 | The use of infosec tools and practices in journalistic contexts

At the time of this writing, the most comprehensive volume dealing with infosec in journalism is Susan E. McGregor's book *Information Security Essentials. A Guide for Reporters, Editors, and Newsroom Leaders* (2021). The book addresses

practitioners who hold various positions in newsrooms of different sizes, offering insights and best practices about infosec in multiple scenarios, from source protection in national security reporting to the coverage of street protests and conflicts. The volume covers strong encryption tools alongside other safety measures, highlighting how infosec in journalism should always be considered from a holistic perspective, not only from a technological software-oriented point of view. According to McGregor (2021, pp. 33–48), threat modeling—the practice of identifying potential adversaries and threats in a case-by-case fashion—has to be considered as the starting point of every discourse on infosec in journalism.

Infosec for journalistic practices is frequently analyzed in the context of the impact of surveillance on the work of journalists or in relation to source protection (Glowacka et al., 2018). The role of the Snowden revelations as a turning point for the practice of journalism is clearly visible in the edited book entitled *Journalism After Snowden* (Bell et al., 2017), where at least two chapters are explicitly dedicated to the protection of journalists' work online in light of surveillance. For instance, journalist Julia Angwin discusses various data protection practices based on her reporting experience (2017 pp. 114–129), while Trevor Timm (2017 pp. 130–141) examines technological solutions for reporters, beyond the email encryption software Pretty Good Privacy (PGP), and the need for newsrooms to create internal practices and teams to deal with infosec, especially in light of the source protection risks involved in leak investigations in the US. Carl Fridh Kleberg (2015) has also published a comprehensive review of digital solutions for source protection with regard to online communication, secure storage of information, smartphone security, and password safety. Source protection in the digital age is also the subject of concern in Julie Posetti's work, *Protecting Journalism Sources in the Digital Age* (2017), published by UNESCO. She notes that Internet surveillance poses existential threats to the practice of investigative reporting and that legal protections for journalists and their sources are frequently ineffective in most countries, indicating encryption as a viable solution, given the amplified risks involved in conducting investigations using digital data (Posetti, 2019).

Overall, surveillance has been indicated as having a potential chilling effect on journalism and as a phenomenon fueling fear and paranoia among journalists (Mills, 2018). In this context, technology-based tactics are considered viable resistance responses to surveillance (Mills & Sarikakis, 2016). Nonetheless, research into journalists' reactions to this state of affairs has been ambivalent. In one of the earliest studies in this area, the Pew Research Center found that, in light of shared concerns about surveillance, many journalists altered their behaviors (2015). Reflecting on the impact of the Snowden revelations and other surveillance-related cases, Paul Bradshaw (2017) has highlighted how regional journalists in the UK have scarcely adopted infosec practices, as well as their limited awareness of infosec in general and the lack of a general threat assessment regarding electronic surveillance. Paul Lashmar (2016) has examined how investigative journalists have changed their attitudes regarding source protection after the Snowden revelations; here, encryption is considered as an indispensable strategy for journalists in the face of digital surveillance, although questions about its efficiency remain unanswered. Stephenson Waters' (2017) study on US national security journalists indicates a general consensus about the difficulties of using infosec tools among journalists, a factor driving adoption resistance. Among the available software, the email encryption software PGP[3] is still the most used, while the open-source whistleblowing software SecureDrop is generally trusted but requires a steep learning curve (Waters, 2017).

Whistleblowing software has been at the center of a series of publications: SecureDrop[4] and GlobaLeaks[5] have been researched in a dedicated book, with the aim of providing a taxonomy of existing whistleblowing platforms in journalism, all created after WikiLeaks' success (Di Salvo, 2020). The current whistleblowing platforms' ecosystem includes organizations of different kinds, from small regional collectives to the most prestigious global newsrooms, such as *The Guardian* and *The New York Times*, underlying the emergence of specific journalistic practices based on the use of encryption. Previously, the origins of whistleblowing platforms and their ties and references to the WikiLeaks experience had been investigated in detail by journalist Andy Greenberg (2012). More recently, Luke Heemsbergen (2021) has examined whistleblowing platforms—or "leaks sites"—in the historical and theoretical context of radical transparency and democracy, pointing at how whistleblowing and leaks may enable new forms of democracy, connecting WikiLeaks to other platforms that followed (2021). In particular, SecureDrop has been analyzed in the

context of its use by English-language mainstream news outlets (Di Salvo, 2021a) and has been indicated as a potential sourcing strategy when it comes to leaks from controversial sources, such as hackers (Di Salvo & Porlezza, 2020). Overall, open-source whistleblowing platforms have also been studied in regard to news outlets' transparency and accountability practices toward sources and the public and in the context of journalistic collaborations (Porlezza & Di Salvo, 2020). Whistleblowing-based journalism has been frequently linked to the use of encryption, as most of the major publications of this kind have been based on leaked materials and data journalism investigations where encryption tools have turned out to be pivotal in coordinating the collaborative work or communicating with the sources. WikiLeaks has definitely been the most visible example of this kind (Lynch, 2010; Zajácz, 2013, etc.[6]). In turn, cross-border collaboration practices have been indicated as fundamental turning points in journalists' adoption of encryption technologies (Heft & Baack, 2021) and constitute one of the areas where they have found adoption in the most comprehensive way (Alfter, 2016), with the "Panama Papers" investigation definitely being one of the most important experiences of this kind (Baack, 2016). The International Consortium of Investigative Journalists, one of the major players in whistleblowing-led journalism, has been analyzed in relation to new political practices that have emerged through digital disclosures in light of its own communication practices, with infosec tools aimed at facilitating secure communications and leak submissions (Heemsbergen, 2018).

Other infosec tools have also gained the attention of media scholars, although less extensively and not necessarily for their security features. Mobile chat apps, such as Signal, Telegram, and WhatsApp, which all offer end-to-end encryption at various levels, have been analyzed in light of how journalists can use them in different reporting scenarios. For instance, Valerie Belair-Gagnon et al. (2017) have examined how foreign correspondents in East Asia use these apps while reporting political unrest situations; secure communication channels offered by such mobile software have been indicated as fundamental assets for communicating with sources who may be victims of surveillance. Similar results have emerged from the analysis of how journalists have covered conflicts in Syria, Yemen, Libya, and Iraq (Christensen & Khalil, 2021). To gain similar security awareness, Syrian local and citizen journalists undergo increased training from diaspora journalists' networks in order to learn how to use encrypted chat messaging apps and other infosec fundamentals (Porlezza & Arafat, 2021). Similar skills training programs are offered by the Institute for War and Peace Reporting, as researched by Mohammad Yousuf and Maureen Taylor (2016). However, the security offered by WhatsApp's end-to-end encryption is still questioned. For instance, Rwandan journalists doubt that it can be trusted in the context of pervasive surveillance and proven usage of spyware by governmental agencies, such as in the Rwandan case (Moon, 2021). Encryption as a safety measure has also emerged from the analysis of ethical reporting practices on the dark web and in relation to covering the drug trade and child sex abuse. In this context as well, whereas encryption has been indicated as a security solution, regular online presence in such a dangerous digital environment could still make journalists vulnerable to anonymous, digital threats (Hognestad, 2021).

Other research in this area has been conducted in a country-specific manner, aiming at analyzing specific infosec strategies adopted by journalists in a variety of countries. For instance, African journalism has been studied in a series of publications. For example, members of the African–Intercontinental investigative journalism networks use groups created on encrypted chat apps, such as Signal and Telegram, to coordinate their collaborative work and apply various email encryption solutions to communicate with international colleagues (Meyer, 2019). Research on the infosec skills and practices of Nigerian journalists shows some awareness about digital threats in the country, but it is limited to the adoption of basic measures, such as the use of strong passwords (Suraj & Olaleye, 2017). In his analysis of Zimbabwean journalists' anti-surveillance attitudes, Allen Munoriyarwa (2021) has argued that encryption tools may be expensive and thus out of reach by newsrooms with limited resources. In Turkey, anti-surveillance practices of activist citizen journalists have been analyzed, pointing at these actors' amateurish—and thus limited—knowledge of the field (Ataman & Çoban, 2018). Two articles have focused on the situation in Slovakia. In a recent paper, investigative journalists' working conditions in the wake of the killing of journalist Ján Kuciak[7] show the journalists' increased use of encrypted communication tools (Urbániková & Haniková, 2021). Previous research in the country had instead highlighted an overall lack of action about infosec by the Slovakian media (Milosavljevič et al., 2015).

3.2 | Motivations, rationales, and organizational issues of infosec in journalism

The articles included in this category have analyzed infosec in journalism mostly by examining how journalists and newsrooms make sense of infosec, their ideas, needs, and the cultural and organizational aspects of these practices. Susan McGregor and Elizabeth Watkins (2016) have investigated how US journalists conceptualize infosec by studying their mental models. They have found how "security by obscurity" is the predominant feature of such models; this implies the journalists' belief that "one need not take particular security precautions unless one is involved in work that is sensitive enough to attract the attention of government actors" (McGregor & Watkins, 2016, p. 39). However, the authors argue that this *forma mentis* is shortsighted, as it fails to acknowledge the various digital threats to which journalists can be exposed in the current digital scenario and even when covering less dangerous or controversial topics and beats. In another research, Watkins et al. (2017) have established that infosec training and sensemaking are mostly lacking in US and French newsrooms and that infosec policies and practices are usually taken over by individual journalists and are again based mostly on the sources' needs. As such, infosec policies are *de facto* delegated to an individual level and constructed mostly around making communication efficient for the sources' ends. Similar results are reported in a 2016 study by McGregor et al., 2016; here journalists express "deference to time, availability, and convenience of sources over security" (p. 424), marking a difference between individual journalists' and organizations' priorities in terms of infosec. The mental models approach has also been applied to research conducted in other geographical areas. For instance, Lokman Tsui and Francis Lee (2019) have analyzed the security mindsets of journalists in Hong Kong, documenting the emergence of three different mental models. The "security by obscurity" model has also been found, together with "security by obfuscation," based on considering some low-tech security solution as efficient in preventing surveillance, and "security as opportunity", applied to journalists with a strong knowledge of infosec and who also recognize its potential values in expanding their reporting opportunities.

Other articles have examined how newsrooms implement infosec practices and tools or which cultures and professional roles drive or facilitate these processes. In investigating journalists' motivations for adopting security technologies, Henrichsen (2019) has found an explicit interest in the protection of journalists' work, stories, and roles connected to the use of infosec tools. According to this study, focused on US journalists and technologists, at the same time, the lack of awareness and security cultures, ambivalence, and uncertainty about infosec tools and practices, as well as the sources' limited knowledge of security, are the most frequent reasons that prevent the adoption of infosec technologies. In her more recent research, Henrichsen has analyzed the crucial role of security champions in supporting the development of security cultures in newsrooms (Henrichsen, 2021). Security champions are defined as individuals who care about infosec and push these issues in the newsroom, without holding a security-dedicated position, contributing to the development of a proper security culture. These figures who mediate between the newsroom and the world of infosec have also been called "technology brokers." Watkins and Anderson have studied these individuals and their influential role of translating, for instance, "the ideas of the encryption community into the needs and meaning-making frames of journalism" (2019). Overall, journalism tends to have different security cultures, which are usually influenced by the beat and employment status of the journalists themselves. Crete-Nishihata et al. (2020) have analyzed these cultures in Canada, finding that journalistic beats directly influence how journalists perceive infosec. In line with previous research results, Canadian investigative journalists also tend to fear state actors and their surveillance capacities more, while non-investigative journalists feel more threatened by non-state actors' actions. Moreover, whereas staff journalists can rely on infosec resources and backing made available by their employers, freelancers benefit from greater autonomy in making infosec decisions but suffer from stronger resource constraints.

4 | FURTHER TRAJECTORIES OF RESEARCH IN AN INCREASINGLY SURVEILLED AND OPAQUE DIGITAL ECOSYSTEM

The 2021 revelations regarding the use of the Pegasus spyware to target journalists around the world have made infosec an even more urgent issue for journalists. Internet surveillance on reporters is rarely conducted for the pure aim of extracting information, but it is usually connected with other monitoring practices or with other ends, such as threatening or silencing journalists. As such, infosec and other anti-surveillance practices are currently among the most urgent issues for journalism freedom at large, as also stated by various organizations dealing with journalism and press freedom. This literature review has underlined the existence of a nascent field of research that, although still limited, is starting to bring up valuable results, especially in understanding which tools and practices are among journalists' first choices, as well as their rationales with regard to adopting infosec. Journalism and media studies have started to analyze how and why journalists rely on infosec to protect and empower their work, a research interest that has gained prominence in the wake of the Snowden revelations. Contrary to other areas of journalism digitalization, infosec is still a highly specialized and niche terrain, characterized by both a strong knowledge barrier entry and evident technical complexity. This is definitely a point that has to be taken into account in analyzing how media and journalism scholars have approached the issue. Despite the emergence of a clear nucleus of literature and of at least two different research patterns discussed here, it can be argued that the amount of research available in this area is surprisingly limited to the one being produced in relation to other highly impactful and systemic phenomena influencing contemporary journalism. As argued by Taylor (2015), journalism still needs a real "paradigm shift" when it comes to infosec and surveillance, because despite important advances since the Snowden revelations, these issues are still frequently neglected or downplayed by journalists and the business at large. A "pivot to security" shift in the business would definitely inspire more research in academia, too. Nonetheless, the currently available literature can still serve as the founding basis for future research patterns.

In particular, further research is needed regarding the most pervasive digital surveillance practices, such as the use of spyware, as well as popular anti-surveillance software and tools, such as Signal, which is increasingly becoming the first choice for secure digital communications in the journalistic field (Shelton, 2021). Moreover, the focus should also be oriented beyond encryption and infosec practices for securing communications, such as digital archiving and securing online accounts, which "complete" infosec in a journalistic context. Most definitely, certain categories of journalists offer interesting perspectives for further research, also beyond investigative reporting. These include journalists who cover mass street protests and movements—where it has been documented that surveillance practices by law enforcement agencies are particularly invasive (Boghosian, 2013, pp. 35–50)—or correspondents from conflict and war frontlines, especially when the use of surveillance technologies (such as military drones, among others) is part of their coverage. Finally, journalists reporting on national security or cybersecurity at large would also be those most exposed to potential surveillance and those with the most sensitive threat models in terms of infosec. Per se, infosec also offers some comparative and multidisciplinary opportunities for research on how journalism is evolving, especially when observing the phenomenon from an international perspective or across different disciplines, obviously starting from computer science and including law and ethnography. More research is likewise definitely needed regarding how journalists relate to infosec in authoritarian regimes or in geographical areas beyond the Western world, where journalism is struggling with even more limited freedom and resources. Overall, a holistic approach to the study of digital threats to journalism is also desirable. Although surveillance is the most dangerous of such threats, it is certainly not the only one. Journalists are harassed, mobbed, threatened, or forced into silence in the digital environment with increasing frequency, also by using other tactics (Waisbord, 2020). This phenomenon has unfortunately targeted female journalists in particular (Westcott, 2019) and has intensified in the context of the COVID-19 pandemic (Wescott, 2020). Finally, this article comes with certain limitations to be taken into account. First, it offers only an overview of the literature available in English; second, it has followed a methodology that may have inevitably lost track of certain publications.

ACKNOWLEDGEMENTS

The Swiss National Science Foundation (SNSF), P2TIP1_191492. Open access funding provided by Università della Svizzera italiana.

ORCID

Philip Di Salvo https://orcid.org/0000-0003-2165-0590

ENDNOTES

[1] Pegasus is one of the most advanced spyware software available, developed and marketed by the Israeli private company NSO Group. Spyware such as Pegasus can be used to target someone's devices in order to put one under surveillance by remotely accessing one's data and monitoring communications transiting through the devices. Although known since 2016, unprecedented details and evidence about Pegasus have emerged in 2021 through the "Pegasus Project" investigation, coordinated by Forbidden Stories, its international media partners, and Amnesty International.

[2] A full list of the Citizen Lab "Targeted Threats" research is available at https://citizenlab.ca/category/research/targeted-threats/

[3] Pretty Good Privacy (PGP) is an email encryption and authentication software that was launched by cryptographer Phil Zimmermann in 1991. It is considered the standard solution for email security until now.

[4] SecureDrop is an open-source software for creating whistleblowing platforms. Currently, the software is managed by the Freedom of the Press Foundation in the US and is used mostly by English-language news outlets (project website: https://securedrop.org/).

[5] GlobaLeaks, also an open-source software for creating whistleblowing platforms, was launched in 2011 by a group of Italian hackers. The software is used by different organizations, including activist groups, nongovernmental organizations (NGOs), media outlets, and public bodies (project website: https://www.globaleaks.org/).

[6] The vast literature about WikiLeaks focuses on various aspects of Julian Assange's organization. Elisabetta Brevini (2017) published a comprehensive literature review.

[7] Ján Kuciak (1990–2018) was a Slovakian investigative journalist who was shot dead in his home together with his partner Martina Kušnírová in February 2018. As Reporters Without Borders wrote following the homicide, Kuciak "specialized in covering large-scale tax fraud for the *Actuality.sk* news website. His last article was about the activities of Marián Kočner, a Slovak businessman with controversial links to several politicians." (2018).

REFERENCES

Alfter, B. (2016). Cross-border collaborative journalism: Why journalists and scholars should talk about an emerging method. *Journal of Applied Journalism & Media Studies*, *5*(2), 297–311.

Anderson, J. M. (2003). Why we need a new definition of information security. *Computers & Security*, *22*(4), 308–313.

Angwin, J. (2017). Digital security for Journalists. In E. Bell, T. Owen, S. Khorana, & J. Henrichsen (Eds.), *Journalism after snowden. The future of the free press in the surveillance state* (pp. 114–129). Columbia University Press.

Ataman, B., & Çoban, B. (2018). Counter-surveillance and alternative new media in Turkey. *Information, Communication & Society*, *21*(7), 1014–1029.

Baack, S. (2016). What big data leaks tell us about the future of journalism - and its past. *Internet Policy Review*, First published on July 26th 2016. https://policyreview.info/articles/news/what-big-data-leaks-tell-us-about-future-journalism-and-its-past/413

Belair-Gagnon, V., Agur, C., & Frisch, N. (2017). The changing physical and social environment of newsgathering: A case study of foreign correspondents using chat apps during unrest. *Social Media + Society*, *3*(1), 1–10. First Published March 27, 2017. https://journals.sagepub.com/doi/full/10.1177/2056305117701163

Bell, E., Owen, T., Khorana, S., & Henrichsen, J. (Eds.). (2017). *Journalism after snowden. The future of the free press in the surveillance state*. Columbia University Press.

Berret, C. (2017). *Newsrooms are making leaking easier–and more secure–than ever*. The Columbia Journalism Review. Retrieved from https://www.cjr.org/tow_center/newsrooms-trump-leaks-secure.php. March 1st

Boghosian, H. (2013). *Spying on democracy*. Open Media Series/City Lights Books.

Bradshaw, P. (2017). Chilling Effect. Regional journalists' source protection and information security practice in the wake of the Snowden and Regulation of Investigatory Powers Act (RIPA) revelations. *Digital Journalism*, *5*(3), 334–352.

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, *3*(2), 77–101.

Brevini, E. (2017). WikiLeaks: Between disclosure and whistle-blowing in digital times. *Sociology Compass*, *11*(3), e12457. https://doi.org/10.1111/soc4.12457

Burnham, D. (1990). Data protection. In M. D. Ermann, M. B. Williams, & C. Gutierrez (Eds.), *Computers, Ethics and society* (pp. 94–105). Oxford University Press.

Carlsson, U., & Pöyhtäri, R. (2017). Words of introduction. In U. Carlsson & R. Pöyhtäri (Eds.), *The Assault on Journalism Building knowledge to protect freedom of expression* (pp. 11–20). Nordicom.

Chadwick, A. (2013). *The hybrid media system: Politics and power*. Oxford University Press.

Christensen, B., & Khalil, A. (2021). Reporting Conflict from Afar: Journalists, Social Media, Communication Technologies, and War. *Journalism Practice*, 1–20. Published online: 05 Apr 2021. https://www.tandfonline.com/doi/full/10.1080/17512786.2021.1908839

Coleman, G. (2019). How has the fight for anonymity and privacy advanced since Snowden's whistle-blowing? *Media, Culture & Society*, *41*(4), 565–571. https://doi.org/10.1177/0163443719843867

Crete-Nishihata, M., Oliver, J., Parsons, C., Walker, D., Tsui, L., & Deibert, R. (2020). The information security cultures of journalism. *Digital Journalism*, *8*(8), 1068–1091.

Di Salvo, P. (2019). *Leaks. Whistleblowing e hacking nell'età senza segreti*. LUISS University Press.

Di Salvo, P. (2020). *Digital whistleblowing platforms in Journalism. Encrypting leaks*. Palgrave Macmillan.

Di Salvo, P. (2021a). Securing whistleblowing in the digital age: SecureDrop and the changing Journalistic practices for source protection. *Digital Journalism*, *9*(4), 443–460.

Di Salvo, P. (2021b). "We Have to act Like our Devices are Already Infected": Investigative Journalists and Internet Surveillance. *Journalism Practice*, 1–19. Published online: 15 Dec 2021. https://www.tandfonline.com/doi/pdf/10.1080/17512786.2021.2014346

Di Salvo, P., & Porlezza, C. (2020). Hybrid professionalism in journalism: Opportunities and risks of hacker sources. *SComS - Studies in Communication Sciences*, *20*(2), 243–254.

Glowacka, D., Siemaszko, K., Smtek, J., & Warso, Z. (2018). Protecting journalistic sources against contemporary means of surveillance. *Northern Lights: Film & Media Studies Yearbook*, *16*(1), 97–111.

Goldberg, I. (2008). Privacy-enhancing technologies for the internet III: Ten years later. In A. Acquisti, S. Gritzalis, C. Lambrinoudakis, & S. De Capitani di Vimercati (Eds.), *Digital privacy. Theory, technologies, and practices*. Auerbach Publications.

Greenberg, A. (2012). *This machine kills secrets. Julian Assange, the cypherpunks, and their fight to empower whistleblowers*. Dutton.

Heemsbergen, L. (2013). Radical transparency in Journalism: Digital evolutions from historical precedents. *Global Media Journal - Canadian Edition*, *6*(1), 45–65.

Heemsbergen, L. (2018). Killing secrets from Panama to Paradise: Understanding the ICIJ through bifurcating communicative and political affordances. *New Media & Society*, *21*(3), 693–711.

Heemsbergen, L. (2021). *Radical transparency and digital democracy: Wikileaks and beyond*. Emerald Publishing Limited.

Heft, A., & Baack, S. (2021). Cross-bordering journalism: How intermediaries of change drive the adoption of new practices. *Journalism*, 1–19. First Published March 19, 2021. https://doi.org/10.1177/1464884921999540

Henrichsen, J. R. (2019). Breaking through the ambivalence: Journalistic responses to information security technologies. *Digital Journalism*, *8*(3), 328–346.

Henrichsen, J. R. (2021). Understanding Nascent Newsroom Security and Safety Cultures: The Emergence of the "Security Champion". *Journalism Practice*, 1–21. Published online: 26 May 2021. https://doi.org/10.1080/17512786.2021.1927802

Henrichsen, J. R., Betz, M., & Lisosky, J. M. (2015). *Building digital safety for Journalism: A survey of selected issues*. UNESCO Publishing. Retrieved from http://unesdoc.unesco.org/images/0023/002323/232358e.pdf

Henrichsen, J. R., & Bloch-Wehba, H. (2017). *Electronic communications surveillance: What Journalists and media organizations need to know*. Reporters Committee for Freedom of the Press. Retrieved from https://www.rcfp.org/wp-content/uploads/2017/05/Electronic_Communications_Surveillance_2017.pdf

Higgins, P. (2020). *How do newsrooms get their news tips? We reviewed over 80 news outlets*. Freedom of the Press Foundation. February 6. Retrieved from https://freedom.press/news/how-do-newsrooms-get-their-news-tips-we-reviewed-over-80-news-outlets/

Hintz, A. (2019). Leaks. In T. P. Vos & F. Hanusch (Eds.), *The International Encyclopedia of Journalism studies*. John Wiley & Sons.

Hognestad, L. I. (2021). Nick, nick. Who's there? Ethical considerations when reporting on the dark net. *Journalism Practice*, *15*(5), 583–600.

Hu, M. (2020). Cambridge Analytica's black box. *Big Data & Society*, *7*(2), 1–6. First Published August 24, 2020. https://doi.org/10.1177/2053951720938091

Human Rights Watch and ACLU. (2014). *With liberty to monitor all: How large-scale US surveillance is harming Journalism, law, and American democracy*. Retrieved from https://www.aclu.org/report/liberty-monitor-all-how-large-scale-us-surveillance-harming-journalism-law-and-american

Jarvis, C. (2021). Cypherpunk ideology: Objectives, profiles, and influences (1992-1998). *Internet Histories*, 1–27. https://doi.org/10.1080/24701475.2021.1935547

Jordan, T., & Taylor, P. A. (2004). *Hacktivism and cyberwars. Rebels with a cause?* Routledge.

Kirchgaessner, S., Lewis, P., Pegg, D., Cutler, S., Lakhani, N., & Safi, M. (2021). *Revealed: Leak uncovers global abuse of cyber-surveillance weapon*. The Guardian, July 18th. Retrieved from https://www.theguardian.com/world/2021/jul/18/revealed-leak-uncovers-global-abuse-of-cyber-surveillance-weapon-nso-group-pegasus

Kleberg, C. F. (2015). The death of source protection? Protecting journalists' source in a post-snowden age. LSE polis. http://eprints.lse.ac.uk/63140/1/__lse.ac.uk_storage_LIBRARY_Secondary_libfile_shared_repository_Content_POLIS_Death%20of%20source%20protection_Kleberg_Death%20of%20source%20protection_2015.pdf

Kubitschko, S. (2015). The role of hackers in countering surveillance and promoting democracy. *Media and Communication*, *3*(2), 77–87.

Lashmar, P. (2016). No more sources? The impact of Snowden's revelations on journalists and their confidential sources. *Journalism Practice*, *11*(6), 665–688.

Lee, M., & Heinrichs, R. (2019). How to protect the truth? Challenges of cybersecurity, investigative journalism and whistleblowing in times of surveillance capitalism. An interview with Micah lee. *Ephemera: theory and politics in organization*, *19*(4), 807–824. http://www.ephemerajournal.org/contribution/how-protect-truth-challenges-cybersecurity-investigative-journalism-and-whistleblowing

Leistert, O. (2012). Resistance against cyber-surveillance within social movements and how surveillance adapts. *Surveillance and Society*, *9*(4), 441–456.

Lynch, L. (2010). "We're going to crack the world open". Wikileaks and the future of investigative reporting. *Journalism Practice*, *4*(3), 309–318.

Lyon, D. (2001). *Surveillance society: Monitoring everyday life*. Open University.

Marczak, B., Scott-Railton, J., Al-Jizawi, N., Anstis, S., & Deibert, R. (2020). *The great iPwn: Journalists hacked with suspected NSO group iMessage 'zero-Click'Exploit*. The Citizen Lab. Retrieved from https://citizenlab.ca/2020/12/the-great-ipwn-journalists-hacked-with-suspected-nso-group-imessage-zero-click-exploit/

Marczak, B., Scott-Railton, J., McKune, S., Abdul Razzak, B., & Deibert, R. (2018). *Hide and seek: Tracking NSO group's Pegasus spyware to operations in 45 countries*. The Citizen Lab. Retrieved from https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/

McGregor, S., & Watkins, E. (2016). 'Security by obscurity': Journalists' mental models of information security. *International Symposium on Online Journalism*, *6*(1), 33–49.

McGregor, S. E. (2021). *Information security Essentials. A guide for reporters, Editors, and newsroom Leaders*. Columbia University Press.

McGregor, S. E., Roesner, F., & Caine, K. (2016). Individual versus organizational computer security and privacy concerns in Journalism. *Proceedings on Privacy Enhancing Technologies*, *2016*(4), 418–435.

Meyer, R. (2019). "Wearing a bullet-proof vest": Social media use in Journalism production within african–intercontinental investigative networks. *African Journalism Studies*, *40*(3), 89–106.

Milan, S. (2013). *Social movements and their technologies: Wiring social change*. Palgrave Macmillan.

Mills, A. (2018). Now you see me – now you don't: Journalists' experiences with surveillance. *Journalism Practice*, *13*(6), 690–707.

Mills, A., & Sarikakis, K. (2016). Reluctant activists? The impact of legislative and structural attempts of surveillance on investigative journalism, *Big Data & Society*, *3*(2), 205395171666938. First published on November 24. https://doi.org/10.1177/2053951716669381

Milosavljevič, M., Amon Prodnik, J., & Kučić, L. J. (2015). Securing the communication of journalists with their sources as a for of source protection - editorial policy of Slovenian media regarding communication and technology. *Teorija in Praksa*, *52*(4), 612–630.

Monsees, L. (2020). *Crypto-Politics. Encryption and democratic practices in the digital era*. Routledge.

Moon, R. (2021). *Moto-taxis, drivers, weather, and WhatsApp: Contextualizing new technology in Rwandan newsrooms*. Digital Journalism, Published online: 21 Jul 2021. Retrieved from https://www.tandfonline.com/doi/full/10.1080/21670811.2021.1929365

Munoriyarwa, A. (2021). When watchdogs fight back: Resisting state surveillance in everyday investigative reporting practices among Zimbabwean journalists. *Journal of Eastern African Studies*, *15*(3), 421–441.

Neumann, P. (1995). *Computer related risks*. ACM Press.

Peltier, T. R., Peltier, J., & Blackley, J. (2005). *Information security fundamentals*. Auerbach Publications.

Pew Research Center. (2015). Investigative Journalists and digital security. Available at: https://www.pewresearch.org/journalism/2015/02/05/investigative-journalists-and-digital-security/

Porlezza, C., & Arafat, R. (2021). Promoting Newsafety from the Exile: The Emergence of New Journalistic Roles in Diaspora Journalists' Networks. *Journalism Practice*, 1-24. Published online: 19 May 2021. https://doi.org/10.1080/17512786.2021.1925947

Porlezza, C., & Di Salvo, P. (2020). The accountability and transparency of whistleblowing platforms issues of networked Journalism and contested boundaries. *Journalism Studies*, *21*(16), 2285–2304.

Posetti, J. (2017). *Protecting journalism sources in the digital age*. Unesco Publishing.

Posetti, J. (2019). The future of investigative Journalism in an era of surveillance and digital privacy erosion. In O. Hahn & F. Stalph (Eds.), *Digital Investigative Journalism: Data, visual analytics and innovative methodologies in International reporting* (pp. 249–261). Palgrave Macmillan.

Reporters Without Borders. (2018). *RSF appalled by investigative reporter's murder in Slovakia*. February 26th. Retrieved from https://rsf.org/en/news/rsf-appalled-investigative-reporters-murder-slovakia

Scott-Railton, J., Marczak, B., Anstis, S., Razzak, B. A., Crete-Nishihata, M., & Deibert, R. (2018). *Reckless VI: Mexican Journalists investigating cartels targeted with NSO spyware following assassination of colleague*. The Citizen Lab. Retrieved from https://citizenlab.ca/2018/11/mexican-journalists-investigating-cartels-targeted-nso-spyware-following-assassination-colleague

Seničar, V., Jerman-Blažič, B., & Klobučar, T. (2003). Privacy-Enhancing Technologies—approaches and development. *Computer Standards & Interfaces*, *25*(2), 147–158.

Shelton, M. (2021). *Signal for beginners. Medium*. Retrieved November 16, from https://mshelton.medium.com/signal-for-beginners-c6b44f76a1f0__;!!N11eV2iwtfs!t0FJP3AUCwHOW7aYVPErwJfndFED1MR9e8unJ9vx2QOOeSYobeeqAQgf32i6X02N2ODSHFCdMLzzkCX4urBIHsFGyJM$

Stamp, M. (2011). *Information security. Principles and practices* (2nd ed.). Wiley.

Suraj, O. A., & Olaleye, O. (2017). Digital safety among Nigerian Journalists: Knowledge, attitudes and practice. In U. Carlsson & R. Pöyhtäri (Eds.), *The Assault on Journalism Building knowledge to protect freedom of expression* (pp. 329–336). Nordicom.

Taylor, P. A. (1999). *Hackers. Crime in the digital sublime*. Routledge.

Taylor, R. (2015). The need for a paradigm shift toward cybersecurity in journalism. *National Cybersecurity Institute Journal*, *1*(3), 45–47.

Thorsen, E. (2016). Cryptic Journalism. News reporting of encryption. *Digital Journalism*, *5*(3), 299–317.

Timm, T. (2017). How news organizations can and must protect reporters and sources at an institutional level. In E. Bell, T. Owen, S. Khorana, & J. Henrichsen (Eds.), *Journalism after snowden. The future of the free press in the surveillance state* (pp. 130–141). Columbia University Press.

Tsui, L. (2019). The importance of digital security to securing press freedom. *Journalism*, *20*(1), 80–82.

Tsui, L., & Lee, F. (2019). How journalists understand the threats and opportunities of new technologies: A study of security mindsets and its implications for press freedom. *Journalism*, *22*, 1317, 1339, First Published May 19, 2019. https://doi.org/10.1177/1464884919849418

Urbániková, M., & Haniková, L. (2021). Coping with the Murder: The Impact of Ján Kuciak's Assassination on Slovak Investigative Journalists. *Journalism Practice*, 1-22. Published online: 25 Jan 2021. https://doi.org/10.1080/17512786.2021.1877179

Waisbord, S. (2020). Mob censorship: Online Harassment of US Journalists in times of digital hate and populism. *Digital Journalism*, *8*(8), 1030–1046. https://doi.org/10.1080/21670811.2020.1818111

Waters, S. (2017). The effects of mass surveillance on Journalists' relations with confidential sources. A constant comparative study. *Digital Journalism*, *6*(10), 1294–1313.

Watkins, E. A., & Anderson, C. W. (2019). Managing Journalistic innovation and source security in the age of the weaponized internet. In A. L. Bygdås, S. Clegg, & A. A. Landsverk Hagen (Eds.), *Media management and digital transformation* (pp. 119–131). Routledge.

Watkins, E. A., Nasrullah Al-Ameen, M., Roesner, F., Caine, K. and McGregor, S. (2017). Creative and Set in Their Ways: Challenges of Security Sensemaking in Newsrooms. Paper presentation, 7th USENIX Workshop on Free and Open Communications on the Internet (FOCI 17). https://www.usenix.org/system/files/conference/foci17/foci17-paper-watkins.pdf

Westcott, L. (2019). *'The threats follow us home': Survey details risks for female Journalists in U.S., Canada." committee to protect Journalists*. Retrieved from https://cpj.org/blog/2019/09/canada-usa-female-journalist-safety-online-harassment-survey.php

Westcott, L. (2020). *NY times reporter davey alba on covering COVID-19 conspiracy theories, facing online harassment. Committee to protect Journalists*. Retrieved from https://cpj.org/2020/05/ny-times-reporter-davey-alba-on-covering-covid-19/

Woodhams, S. (2021). *Spyware: An unregulated and escalating threat to independent media*. Center for International Media Assistance. Retrieved from https://www.skeyesmedia.org/documents/bo_filemanager/CIMA_Spyware-Report_web_150ppi.pdf

Yousuf, M., & Taylor, M. (2016). Helping Syrians tell their story to the world. Training Syrian citizen journalists through connective journalism. *Journalism Practice*, *11*(2–3), 302–318.

Zajácz, R. (2013). WikiLeaks and the problem of anonymity: A network control perspective. *Media, Culture & Society*, *35*(4), 489–505.

AUTHOR BIOGRAPHY

Philip Di Salvo is a post-doctoral researcher at Università della Svizzera italiana (USI)'s Insitute of Media and Journalism. Currently, he is a Visiting Fellow at the London School of Economics and Political Science (LSE)'s Department of Media and Communications. Philip does research about whistleblowing, investigative journalism, internet surveillance and the relationship between journalism and hacking.

How to cite this article: Di Salvo, P. (2022). Information security and journalism: Mapping a nascent research field. *Sociology Compass*, e12961. https://doi.org/10.1111/soc4.12961