Volume 12 Number 7 September 2024

Digital Journalism

DIGITAL JOURNALISM

Routledge Taylor & Francis Group

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

Dealing with the Black Box: European Journalists and the Threats of Spyware

Philip Di Salvo

To cite this article: Philip Di Salvo (21 Jul 2024): Dealing with the Black Box: European Journalists and the Threats of Spyware, Digital Journalism, DOI: 10.1080/21670811.2024.2378122

To link to this article: https://doi.org/10.1080/21670811.2024.2378122

Published online: 21 Jul 2024.

DIGITAL JOURNALISM
https://doi.org/10.1080/21670811.2024.2378122

Routledge
Taylor & Francis Group

RESEARCH ARTICLE

Dealing with the Black Box: European Journalists and the Threats of Spyware

Philip Di Salvo

School of Humanities and Social Sciences (SHSS), Universität St. Gallen, St Gallen, Switzerland

ABSTRACT

Revelations from the 2021 "Pegasus Project" investigation into the use of spyware have confirmed long-held concerns about the proliferation of the technology as a surveillance solution to monitor the activities of journalists around the world. Spyware is a particularly malicious form of malware that can potentially expose a target's entire digital life, sometimes even leaving victims powerless to prevent an attack. As such, spyware appears to be the ultimate tool of oppression that can be used against journalists, and its proliferation is currently taking place with extremely limited transparency and according to "black box" dynamics. The aim of this paper is to shed light on how spyware technology can affect the work and security of journalists by analyzing what threats spyware poses to the practice of journalism. Qualitative and exploratory in nature, and theoretically grounded in surveillance studies and the growing body of literature on information security in journalism, the article is based on a series of qualitative interviews with technologists and reporters conducted to deepen the understanding of the threats posed by spyware and to provide an overview of potential resistance and neutralization practices that journalists can put in place, as well as their effectiveness. Overall, the article aims to contribute to the study of the impact of surveillance on journalism and its implications for press freedom.

KEYWORDS

Spyware; information security; surveillance; journalism safety; hacking; source protection

Introduction

In 2021, the "Pegasus Project," an investigation into the use of spyware to conduct digital surveillance against various individuals and organizations, shed further light on how spyware was being used by a range of actors to monitor the online activities of journalists (Forbidden Stories 2021). Spyware and its use against the press had been documented before (Deibert 2013 – among others), but the "Pegasus Project" revelations brought unprecedented evidence of the phenomenon. According to the investigation, at least 180 journalists worldwide were selected as potential targets using the Pegasus spyware, and it is possible that the estimated number is higher (Pegg et al. 2021). Spyware must be considered among other authoritarian practices

CONTACT Philip Di Salvo philip.disalvo@unisg.ch

that undermine democratic values in the digital sphere (Glasius and Michaelsen 2018) and perhaps the most intrusive and dangerous form of surveillance targeting journalists (Committee To Protect Journalists 2022). The use of spyware poses serious problems for journalists because, if targeted, their digital lives, work and sources can be exposed by actors who may have an interest in spying or monitoring their activities and even, in many cases, stopping or silencing them, combining digital and physical attacks.

Theoretically grounded in journalism and surveillance studies and the conceptualization of the "surveillant assemblage" (Haggerty and Ericson 2000; 2016), this article aims to shed light on the threats and particularities of spyware when it comes to its use against journalists. The article focuses on the perspectives and views of journalists and technologists who have worked with spyware, either through support, training in information security, or by investigating the surveillance market or the use of spyware against journalists themselves. The article discusses findings and perspectives from Europe, with the aim of helping to fill a geographical gap in this area of research. Research on the impact of digital surveillance on journalism is still a niche area, and despite the global impact of the "Pegasus Project" and other revelations, research on the specific threats of spyware to the practice of journalism is still extremely limited, especially when it comes to Europe (Di Salvo 2022). At the same time, the paper will use spyware as a lens through which to discuss contemporary surveillance and black-boxing dynamics and their implications for journalism and press freedom.

Spyware, a "Surveillant Assemblage" and Its Use against Journalists

Spyware is a "class of software that is surreptitiously installed on a user's computer and monitors a user's activity and reports back to a third party on that behavior" (Stafford and Urbaczewski 2004, 292). Today, spyware can be installed on a variety of devices, and smartphones have become the most targeted of these devices due to the wealth of different data they can store (Perlroth 2021: 177-189). Spyware can be installed and operated with different technical strategies and levels of sophistication (McGregor 2021: 65) to infiltrate target devices and extract information, data and communications in transit or stored on the infected devices. As such, spyware encapsulates the diverse and pernicious characteristics of contemporary surveillance, particularly when it comes to technical specifications and the dynamics of invisibility. A framework for understanding the complexities and ramifications of spyware is an "ecological" one that aims to consider all of its "machinations, concrete and abstract," encompassing technological, social, psychological and economic parts (Parikka 2016: xxviii). Given this ecological nature, spyware can also be considered as a "surveillant assemblage" (Haggerty and Ericson 2000) in its own right, the significance of which becomes apparent when it is analyzed together in its technological, practical, and political-economic components. In this paper, spyware will be considered both as part of the broader contemporary "surveillant assemblage" and as an assemblage itself. This means that spyware will be considered both as a key factor in the way surveillance works today and, in parallel, as a socio-technical structure composed of different elements that can only be understood by analyzing their complex interrelationships beyond technical details. All these elements become particularly clear

when spyware is analyzed in terms of how it threatens the practice of journalism, a lens that is particularly effective in bringing these elements to the fore.

Drawing on the work and concepts of Gilles Deleuze and Félix Guattari, Kevin Haggerty and Ericson (2000) argue that the notion of the "surveillant assemblage" refers to surveillance not as a static phenomenon, but as an evolving and active process shaped by a variety of factors and actors (Haggerty and Ericson 2000: 606). Moreover, the "surveillant assemblage" is not just a collection of discrete elements, but a dynamic and constantly evolving system shaped by a wide range of political, economic, social, and cultural forces. Thus, assessing the impact of spyware on journalism allows us to deconstruct the various components that make up the core of spyware and to understand how the technical specifications work together with various non-technical characteristics, both of which are clearly visible in the way they threaten journalists. In the context of this paper, spyware is seen not just as a matter of technology, but as a socio-technical system shaped by social norms, cultural values, and power relations. Furthermore, as will be discussed further in this paper, the spyware's assemblage of software, hardware, and practices can also be seen as most revealing of the characteristics of contemporary surveillance and its practices of "obfuscation" and "blackboxing" (Brunton and Nissenbaum 2015; Latour 1992).

Researchers, activists, and journalists have played a key role in exposing the details of spyware use. Citizen Lab has been researching the issue for more than a decade, doing forensic work to map the proliferation of spyware against political targets, including journalists. As early as 2009, Citizen Lab tracked the Chinese GhostNet espionage operation launched against the Dalai Lama using the Ghost RAT spyware (Deibert 2013: 23-27; Information Warfare Monitor 2009). Since these early cases, the use of spyware has proliferated, making the technology one of the solutions of choice for the surveillance of journalists as well. This has been documented at least in Ethiopia (Citizen Lab 2014), the United Arab Emirates (Deibert 2020: 150) and Mexico (Citizen Lab 2017). The most well-known and analyzed spyware is Pegasus, produced by the Israeli NSO Group. In 2018, Citizen Lab was able to confirm the use of Pegasus in 45 countries (Citizen Lab 2018). In 2021, however, the network of media partners involved in the "Pegasus Project" was able to reveal unprecedented details about the use of spyware internationally, including attacks on the press in India, Mexico, Hungary, Morocco, and France, among others (Forbidden Stories 2021). Revelations about the use of the Pegasus spyware continued into 2022, particularly its widespread use in Spain (Farrow 2022) and Mexico (R3D 2022). Pegasus and NSO – its Israeli producer – are by no means the only recent cases, and other companies and software have been exposed in recent years. The Italian company Hacking Team was the target of a "public interest hack" (Coleman 2017) that resulted in the leak of its internal data and source code already in 2015. Similarly, the Anglo-German company GammaGroup suffered a leak resulting from a cyberattack in 2014 that exposed the details of its FinFisher spyware. In both cases, the hacktivist (or hacktivist collective) Phineas Fisher claimed responsibility (Burkart and McCourt 2017).

The market of surveillance tools and the large number of companies involved is one of the crucial components of the spyware "surveillant assemblage" (Haggerty and Ericson 2000) and one of the most descriptive, especially when it comes to the secrecy

and invisibility of the technology and its "black box" characteristics. Despite the lack of transparency, the business is growing, and the technology is undergoing a process of "commodification" (Harkin, Molnar, and Vowles 2020), while potential users are also expanding beyond governments and intelligence agencies to potentially include non-state actors (Workneh 2022). This has been made possible by the equally growing shadow market for technological vulnerabilities and exploits, which has led to an "arms race" for cyberweapons and the trading of ready-to-exploit vulnerabilities in the security of technological hardware and software (Deibert 2013: 15-18; Perlroth 2021). In particular, "zero-day" vulnerabilities, those security flaws in commercial software and hardware that are unknown even to their manufacturers, are the most sought-after by surveillance companies, as they can be exploited to launch attacks with spyware that can be installed with "zero-click" attacks, which bypass the security of devices without requiring targets to do anything to become infected, as is the case with phishing emails and text messages, or "spearphishing" attacks (McGregor 2021: 63). Historically, one of the first instances where a "zero day" exploit was used to launch a hacking attack is usually considered to be the 2009 US and Israeli-led cyberattack against the Iranian nuclear enrichment facility in Natanz, which was targeted with the Stuxnet malware (Zetter 2015).

As will be discussed later in this article, what began as a potential cyberwar strategy for state actors has since spread to other private and smaller manufacturers. NSO's Pegasus could be remotely installed on target devices through a "zero-day," "zero-click" exploit against iMessage, the iPhone's default SMS app. The vulnerability was discovered during forensic analysis of a Saudi activist's phone (Citizen Lab 2021). As a result, Apple – unaware of this vulnerability – released a security update and patch in September 2021 (Mihalcik and Fowler 2021). Journalists are an ideal target for spyware because the technology has the potential to compromise some of the profession's most important foundations and ethical principles, such as confidentiality, protection of sources and autonomy. As such, it is precisely when used to target journalists that spyware demonstrates its full potential and significance, not only as a specific "site" of surveillance (Lyon 2007: 25), but also as a symbolic demonstration of how surveillance in general operates today, largely by exploiting the features and weaknesses of digitization itself and its infrastructures (Westlund, Krøvel, and Orgeret 2022).

Surveillance of Journalists and Information Security

Installing spyware on targets' devices is part of what David Lyon defines as one of the three main layers of contemporary digital surveillance, along with intercepting data in transit and accessing stored data (Lyon 2015: 17-21). To date, the existing literature has largely focused on how journalists can respond to the pressures of digital surveillance. For example, this corpus of publications has focused on source protection, showing how surveillance threats require a rethinking of journalistic practices and the adoption of encryption technologies (Lashmar 2016; Posetti 2017). When it comes to adopting anti-surveillance practices and solutions, journalists again seem to make their decision mostly based on the needs of their sources, rather than their own or those of their organizations or employers (Watkins et al.

2017) and on the basis of tools fitting existing workflows and their necessity for collaborations (McGregor et al. 2017). When it comes to the impact on journalists' activities, research has produced mixed results: for example, US investigative reporters seem to have partially changed the way they work in light of digital surveillance (Pew Research Center 2015). In contrast, UK journalists seem to have little or no awareness of these dangers and the solutions provided by encryption (Bradshaw 2017). In particular, when it comes to protecting sources, the adoption of security practices and encryption tools for anonymity is now so central that it's also integrated into the identity of investigative journalists and their roles (Biscop and Décary-Hétu 2022).

Digital surveillance has also been analyzed as a factor that generates fear and a sense of paranoia among journalists: this sense of insecurity is a crucial factor in the wider "chilling effect" on journalists' freedoms and liberties (Mills 2019). European investigative reporters have also identified the stealthy and unknown elements of internet surveillance as the most worrying, pointing to phishing attacks as one of the most threatening surveillance strategies (Di Salvo 2021). Overall, research has confirmed the prevalence of a "security by obscurity" mental model among journalists (McGregor and Watkins 2016; Tsui and Lee 2019; Henrichsen 2020). According to this view, journalists are convinced that information security should only be a concern for those dealing with sensitive issues or those reporting on high-level actors with surveillance capabilities. However, security cultures are diverse and usually influenced by different factors (Crete-Nishihata et al. 2020; Henrichsen 2022). Differences in how surveillance affects the work of journalists are also linked to the strength of democracy: for example, in contexts where democratic oversight of the actions of intelligence agencies is limited, such as in Pakistan, the impact on journalists' well-being and work is inevitably direr (Jamil 2021).

However, journalists can also be affected by surveillance in democratic contexts, often through the abuse of surveillance powers granted under security legislation (Harkin and Mann 2023). Research has also shown that journalists can take a fatalistic approach to internet surveillance, tending to view their communications as *de facto* subject to potential surveillance, regardless of their efforts to protect their devices and data. This has been shown in research on Mexican journalists (González and Rodelo 2020) and again on European journalists (Di Salvo 2021). Overall, the impact of spyware on journalists has not yet been extensively studied from a journalism and media studies perspective. The most comprehensive research in this area is Samuel Woodhams (2021) report for the Center for International Media Assistance (CIMA), which identified spyware as one of the most immediate threats facing journalism in a context of increased political pressure. But looking at the research that has analyzed journalists' exposure to digital surveillance, two core issues seem to emerge. First, the fear that the protection of sources – arguably the most important ethical concern for journalists – could be compromised. Second, there is a great deal of uncertainty about how surveillance could be used against journalists, by whom, and according to what strategies. This could apply to various forms of digital surveillance, but these points are even more central when it comes to spyware, the design and conceptualization of which is based on these assumptions. In this light, spyware embodies the most central elements of the functioning of contemporary surveillance and its various

"assemblages," and as such is potentially the most dangerous digital threat to journalists, as spyware can jeopardize all three dimensions in which journalistic security should be enacted: in its own infrastructures; in its practices (i.e., source protection); and in the consequences faced by journalists (psychological, social and political) (Westlund, Krøvel, and Orgeret 2022).

Methodology and Research Design

This paper is based on 14 semi-structured qualitative interviews conducted in the autumn of 2022 with technologists and journalists working for European-based organizations. The interviews were conducted *via* Zoom and lasted on average around 40 minutes. Interviewees were included in the sample either because of their experience reporting on the use of spyware or because of their expertise in information security as applied to journalism. As a result, the interviewees represent a range of organizations, from investigative or technology-focused news brands to human rights and digital rights NGOs. To identify interviewees, a list of relevant organizations was initially drawn up. Later, individuals responsible for cyber or information security issues were identified on the organizations' websites or on X. Non-journalistic organizations were selected for their involvement in recent research and advocacy on spyware, while news organizations were selected for having published investigations and analysis on these issues between 2020 and 2022. Technologists were included in the sample because of their knowledge of the technical and ethical implications of spyware for journalism or their direct work in helping reporters and news organizations establish information security practices.

Due to the sensitivity of the issue and the specific threat models of the interviewees, the individuals included in the sample were granted complete anonymity. As some of the interviewees also requested that their nationality be withheld, the same level of confidentiality was granted to the entire sample. Some information about the interviewees' affiliations and backgrounds is still available in Table 1. Interviews were initially transcribed using the automated software Sonix.ai and later edited manually by the author for linguistic and stylistic accuracy. The transcripts were analyzed using inductive thematic analysis, which aims to identify the main themes in

Table 1. Interviewees details.

Interviewee	Orgnization	Role	Background
1	Specialized newsroom	Editor	Journalism
2	Human Rights NGO	Head of Security	Technology
3	Human Rights NGO	Deputy Director	Policy
4	Journalism education	Consultant	Technology
5	General interest newsroom	Journalist	Journalism
6	Digital Rights NGO	Security Incident Handler	Technology
7	Specialized newsroom	Director	Journalism
8	Journalism non-profit	Trainer	Technology
9	Digital Rights NGO	Digital protection coordinator	Technology
10	Specialized newsroom	Chief Technology Officer	Technology
11	Specialized newsroom	Consultant	Technology
12	Specialized newsroom	Chief Technology Officer	Technology
13	Freelance	Journalist	Journalism
14	Freelance	Researcher	Policy

the interviewees' responses, following an inductive approach (Braun and Clarke 2006, 83). The analysis of the interviews was carried out with the help of NVivo software, which was used for the coding process. The analysis of the transcripts allowed the identification of 40 original codes, which were later merged into larger and more focused codes ($n = 24$). This operation of merging and reduction was carried out to simplify the constellation of codes and to avoid overlap and repetition, especially in cases where the codes emerged from a limited number of interviews. These codes were used as a starting point for identifying the general themes, which were intended as "the most salient constellations of meaning present in the interview transcripts" (Joffe 2012, 209).

Five main themes emerged from this second level of analysis. Overall, the five themes relate to the threats posed by spyware, the most vulnerable areas of journalistic work involved, the identity and nature of potential attackers, the uncertainties surrounding spyware technology and the strategies journalists can adopt to mitigate the dangers posed by these technologies. The five themes identified are 1) *The different dimension of jeopardized journalism safety*; 2) *Spyware technology is "hard to see"*; 3) *A global and untraceable proliferation*; 4) *The unresolved dilemma of "being a target"*; 5) *Digital hygiene as a mitigation strategy*. Details of the codes included in each theme are given in Table 2.

Table 2. Themes details.

Themes	Frequency (references in interviews)
1) The different dimension of jeopardized journalism safety	41 (total)
Invasion of digital life	18
Source protection	12
Psychological effects	7
A threat parallel to others	4
2) Spyware technology is 'hard to see'	72 (total)
Technological invisibility	19
Zero clicks attacks, vulnerabilites and exploits	19
Potential journalistic counter-attacks	18
Exploitation of technologies peculiarities	10
Lack of knowledge in the journalistic field	6
3) A global and untraceable proliferation	81 (total)
The expanding spyware market	25
Peculiarities of spyware use in authoritarian regimes	21
Global diffusion beyond authoritarian regimes	18
State and private actors overlapping	13
Dangers of legal surveillance	4
4) The 'being a target' unresolved dilemma	34 (total)
General threat to everybody	16
Spyware attacks a concern for specific targets	9
Resources needed for launching spyware attacks	6
Journalists as explicit targets	3
5) Digital hygiene as a mitigation strategy	66 (total)
Importance of digital hygiene	24
Information security specific practices	11
Threat modelling	8
Nothing can be done against spyware	11
Encryption still helps	7
Encryption is important but it can't be of help	5

Results

1) The Different Dimension of Jeopardized Journalism Safety

Spyware poses several major security threats when used against journalists. These threats have different dimensions, both professional and personal. In most cases, they cited the protection of sources as the most pressing concern, linking the use of spyware to the potential exposure of their sources. Source security is usually mentioned before the personal security of the journalists themselves. Overall, the interviewees expressed very similar and straightforward views:

> "This is a further problem for journalists, because obviously, given their work, such a violation compromises also the relationship with the sources and compromises the safety of the sources themselves."
>
> (Interviewee 1)

Spyware also concerns respondents in terms of the large-scale invasion of privacy that the technology can cause. Respondents spoke clearly about the potential invasion of their entire digital lives. In this case, respondents emphasized the stark difference between the capabilities of spyware and other, less omnipresent surveillance practices designed to intercept a single area of their digital lives, rather than potentially all of them together:

> "It literally takes all the data about the system, which is absolutely terrifying because your devices will pretty much contain your whole life. It will infiltrate your device, which will contain your personal life, your professional life, and your meetings with sources, or your notes."
>
> (Interviewee 8)

This total invasion of privacy is also linked to the potential risk of doxing of personal information and data, and the psychological effects this can have:

> "I think the lack of privacy and the continued harassment and following also has deep psychological impacts on people working in hard environments, right?."
>
> (Interviewee 10)

Respondents also pointed to psychological effects not directly related to effective attacks, but rather to the various uncertainties created by spyware. This stems from the feeling of not being able to verify a potential attacker's access to the technology, or the impossibility of obtaining proof of being under surveillance or not. All these unresolved dilemmas create a sense of paranoia among journalists, which directly contributes to jeopardizing their safety and well-being. In sum, spyware technology can have a chilling effect without directly targeting journalists:

> "There are two things that immediately come to mind. One is the psychological impact of being targeted for surveillance or even believing that you could be targeted for surveillance. There is this sort of crazy false narrative around surveillance, where it's like there's no harm unless you can prove you've been hacked. And that is just not accurate."
>
> (Interviewee 3)

Psychological consequences are certainly severe for direct victims of spyware attacks, both also for those journalists constantly exposed to unverifiable surveillance threats. Interviewees with experience in assisting victims of spyware attacks confirmed these dire physiological effects:

> "You get exposed by people who have complete mental breakdowns because they begin to realize the extent of the problem. The media must take this kind of thing more seriously and understand that there is work to be done on developing their technical knowledge of preparation and response to these kinds of threats, which cannot be just relying on that handful of technologists who who have been working on this for the past five years and check a cell phone once in a blue moon. There must be a more systematic procedural and educational development."
>
> (Interviewee 2)

2) Spyware Technology is "Hard to See"

Spyware technology has been described as secretive and stealthy, similarly to several algorithmic technologies that have also been defined as "hard to see" (Crawford and Whittaker 2016). This opacity stems from the technical characteristics of spyware, which are designed to be difficult to trace. As a result, journalists are deterred by the constant sense of uncertainty that they may be targeted without having the means to verify this, or that they may be targeted during sensitive investigations. This can leave a serious power imbalance in the hands of potential attackers:

> "If my phone does not give me any sign, then it's hard for me to guess until there is really a big issue and people start to be arrested or start to be prosecuted. This is what I think modern journalists are really facing now."
>
> (Interviewee 6)

Detecting spyware on a smartphone can only be done through technical and forensic analysis that cannot be performed by the targets themselves and cannot be done under normal working conditions. Of all the invisibilities of spyware, the most discussed were those associated with the most advanced attack strategies. For example, respondents expressed concern about "zero-click" attacks. This is the most controversial and dangerous feature of spyware, as it leaves targets with no obvious lines of defense and no deterrent. These attacks are made possible by the proliferation and growth of the "zero day" exploit market, which makes them even more difficult to detect, but more effective:

> "One of the techniques for a long time has been to let targets click on a link that led to the spyware to be downloaded in the phone, right? That's the old technique. What NSO brought up as a company, it's a totally new concept: 'zero click'. Here, I only need to find a bug on an app or on the operating system. It will be easier for the attacker; I don't need them to click on anything. So, this is how new things happen. It started three or four years ago. This is one of the things that actually brought a huge change in the spyware industry."
>
> (Interviewee 6)

Phishing emails and other similar attack strategies, which still require some action by the victim, can be considered less sophisticated compared to "zero days" attacks. Nevertheless, it is important to note that these attacks continue to be carried out on a larger scale and are a common attack scenario, including targeting journalists who have shown a high level of interest in them (Di Salvo 2021). The use of "zero-click" attacks also makes spyware detection and attribution more complex. As a result, the invisibility of the technology is reinforced by the opacity of the spyware market itself:

> "We really saw that NSO started to rise around 2015 or 2016 and became super effective at it because, first of all, they have really good ways to hack into a phone because they work with various companies around the world to buy the zero days which they integrate into their products. And it seems to be really effective, and it's hard for even, you know, Amnesty Technology and Citizen Lab, to look at forensic cases of hacks […]. You see that they have a tough time to really get a lot of information. And so it's a really effective strategy."
>
> (Interviewee 11)

3) A Global and Untraceable Proliferation

Somewhat in continuity with the previous "invisible" impact of spyware, its proliferation has also been described as difficult to track, monitor and opaque (Deibert 2022). This is evident in several areas: the industry producing the technology, the geographical spread of spyware use, and the nature of potential attackers. Despite recent journalistic scoops and revelations, many elements of the surveillance market remain unknown, starting with the capabilities of smaller companies that operate in even more controversial ways and are difficult to monitor, especially those operating in the "hacking for hire" sector, where companies provide both the technology and the operations needed to attack targets:

> "There is a whole world of spyware, which is maybe a little more low-level, as well as operating in an even grayer area. We have also seen, in India and in other places, companies that are basically just 'hacking-for-hire'. This kind of reality is also growing and in a more disordered way, but this thing is already here."
>
> (Interviewee 1)

Some interviewees stressed that the exposure of NSO and Pegasus in 2021 should not create a false analogy that the spyware industry is only about big companies. According to this research, the reality is different and may be more subtle (and larger):

> "There is a risk that we think that NSO is a kind of exception. I think there's probably hundreds of companies that are offering similar capabilities. […] They're using different languages and different ways of describing it, whether it's offensive cybersecurity or interception methods. But the result is that they're kind of selling very similar capabilities."
>
> (Interviewee 14)

Interviewees also highlighted the overlap between state and private actors as potential users of spyware. They cited uncertainties about the potential for private

actors to acquire tools that were previously only available to state actors, and the consequent expansion of the use of spyware by corporations or businesses:

> "I think that unless regulation and some sort of structural changes are implemented within the commercial side of things, then there is a genuine risk that private actors and companies could get hold of this sort of technology. And I think they probably already do to a certain extent, but it certainly hasn't been the focus of a lot of the reporting over the last 12 months or so."
>
> (Interviewee 14)

In countries where there is a weak demarcation between the powers of the state and those of private actors, the interplay between the two has been observed in the use of spyware, due to the weak separation of powers that tends to characterize non-democratic countries. This can lead to an even greater lack of transparency, where some "proxy" dynamics may also be at play in the spyware business:

> "But in some countries, there is no real gap between the private and governmental sectors, right? So governments can buy it and just give it to people in the private sector and they can use it, so they don't get backlash or legal procedures against them. Other governments in the MENA area, like the United Arab Emirates, for example, give that spyware and support hacking to other countries, like Egypt, for example. So, there is also a kind of proxies happening on this, through proxy governments or customers that buy it and proxy it to another party and that party is then using it."
>
> (Interviewee 9)

In terms of the geography of spyware, interviewees spoke of fears that the technology could now be used beyond authoritarian regimes and in democratic contexts, as confirmed by the recent revelations of the "Pegasus Project," which clearly implicated Hungary and Spain, two EU member states:

> "In my opinion, yes, some examples are obvious: and the one of Hungarian journalists involved in reporting activities towards politicians is a clear example of how this type of risk has already arrived within the European perimeter."
>
> (Interviewee 13)

However, the use of spyware by authoritarian regimes poses a more dangerous threat to journalists, according to most respondents. In these countries, protections for journalists are even weaker or non-existent, and impunity is rampant, as are links between government agencies and powerful private actors:

> "Some journalists are based in countries where they already face a lot of threats, traditional threats, non-digital threats, together with usual traditional spying or traditional pressure from politicians or from the police. For them, the digital threat is just another layer of danger, I think. For journalists operating in, for example, Mexico, we have a lot of examples of the use of Pegasus against journalists, against dozens of journalists."
>
> (Interviewee 5)

Finally, another vector for the further spread of spyware has been identified in leaks, as the source code of spyware can be distributed online, making it available to unofficial users who could access (or replicate) similar software:

> "We should not also ignore the risk that those spyware or their codes could be leaked any time. I saw a lot of mighty tools of spyware that got their codes leaked and that was then used to compromise desktops and servers, and I wouldn't be surprised that, uh, spyware like Pegasus could be leaked anytime soon."
>
> (Interviewee 6)

4) The Unresolved Dilemma of "Being a Target"

When it comes to journalists being targeted by spyware, respondents had different views on who should be concerned. For example, some respondents stressed that all journalists could potentially be hacked by spyware. Some interviewees emphasized that the most advanced spyware, such as Pegasus, is only part of an ecosystem that also includes less advanced, more accessible products that could be used to target journalists in less controversial and dangerous circumstances or in lower profile contexts. For example:

> "The notion of the 'dissident' or of the 'million dollar journalist' is completely wrong. These tools are obviously advanced – not all but some are – and they cost a certain amount of money and are not necessarily within everyone's reach, because there is an investment to be made. But the thing that needs to be understood is that this investment is very easily dissipated. You don't spend 2 million dollars to target a single person, you spend that money to acquire a capability. That capability is then reused horizontally, so even people who are not necessarily of the highest profile very often find themselves targeted for the most futile and banal reason."
>
> (Interviewee 2)

For some other respondents, however, only a limited number of journalists should be concerned about becoming targets of spyware attacks. A few factors influence this discussion, including the beat covered and the connection to certain highly sensitive issues, such as national security or government abuse, or the democratic status of the journalist's nationality:

> "Well, in theory, everyone is potentially a target because the software doesn't discriminate against its targets. The users of the software do discriminate, though. Obviously, if you're working on national security or if you are a journalist in an authoritarian regime trying to uncover some government secrets, yeah, obviously you're a bigger target than a sports journalist, for example."
>
> (Interviewee 5)

While the number of potential victims of spyware attacks is ideally smaller according to these respondents, their comments should not be seen as dismissive of surveillance risks: all these comments relate to the likelihood of a direct, targeted spyware attack and should not be seen as a general comment on the wrongness of the technology, its proliferation and its dangers.

5) Digital Hygiene as a Mitigation Strategy

When it comes to the strategies and practices journalists can adopt to protect themselves from spyware, respondents see digital hygiene as a viable solution. However,

there is general agreement that these strategies can only mitigate the consequences of attacks, not prevent them. This is especially true in the case of "zero-click" attacks, for which there is no specific information security tactic. According to the interviewees, all these mitigation steps are related to what is commonly referred to as "digital hygiene" (Dharampal 2021), a set of practices that includes basic activities such as keeping devices and software updated, compartmentalizing the use of devices, and being aware of some of the most common attack strategies:

> "There is too much disproportion between your skills and those of your opponents: the only thing you can do is, if you think you are at risk, is to segment devices and accounts, use phone numbers, devices and accounts that are little known. That is, if your phone or device you do everything with is very well known, maybe don't use it to have a conversation with your Snowden. You will have to segment and compartmentalize as much as possible, to confine the most sensitive things to some devices that you will use only for that and that I would try to use for no other activity."
>
> (Interviewee 1)

It's important to note that, as with medical hygiene, digital hygiene cannot be effective as a direct line of defense against very aggressive and virulent viruses. This is also the case with the most sophisticated spyware, which is created using "zero day" vulnerabilities and can be used to target software or hardware that can't be technically secured. The use of different setups and devices could, through compartmentalization, make an attack line more complex to identify or limit the exposure of sensitive information to a smaller number of potential entry points:

> "What can we do to protect ourselves from Pegasus? There is little you can do because we have seen that even on very recent versions of iOS you might still be vulnerable. So what we usually say in terms of updating your software, of course, it still holds as an important thing to do, but it's not necessarily enough. Still, this teaches us the importance of digital hygiene because, for example, one protection or one safeguard against that could be compartmentalization, which is using different devices for different projects or at least to distinguish between your personal life and your working life."
>
> (Interviewee 4)

The most comprehensive defenses journalists can adopt against spyware are not based on technical solutions, but rather on operational security practices designed to make attacks more difficult to execute:

> "There are some small precautions that perhaps can reduce some risk elements, such as disabling some features or some applications that we know are particularly used for this kind of attacks, such as disabling iMessage or disabling JavaScript in Safari. It is really up to small precautions of this kind, but they are only bulwarks to a problem that you cannot completely solve with purely IT precautions. The most important thing to think about is from an operational point of view."
>
> (Interviewee 2)

At the heart of any information security and digital hygiene strategy is an effective threat modelling assessment (McGregor 2021: Chapter 3), something that interviewees said all journalists should consider when starting to think about surveillance and spyware. Interviewees mentioned threat modelling to emphasize the importance of

context in identifying potential surveillance threats. While the basics of digital hygiene are the same for everyone, other more sophisticated information security practices should only be implemented after a contextual, individual, and targeted threat assessment:

> "Risk is incredibly context specific, so I wouldn't say that there is a single crucial thing that can be done. It also very much depends on the journalist's security procedures, right? If, for example, you're communicating with sources and you use disappearing messages and you use, for example, pseudonyms for all your sources and you're very, very careful, then maybe that much source data cannot leak out, but it's all incredibly context dependent."
>
> (Interviewee 8)

Digital hygiene and information security practices also included a discussion of the potential benefits of encryption as a defense strategy. When it comes to encryption, respondents identified some specific practices and tools that journalists can adopt in this regard. These include virtual private networks (VPNs) and encrypted chat applications. When it comes to the effectiveness of encryption as a protection strategy against spyware, respondents were divided. All respondents agreed that cryptography has clear security benefits, but some also pointed out that even the most advanced encrypted communications or storage applications can do little or nothing to directly protect journalists from spyware, as the technology has the ability to bypass such security protocols and allow remote access to a compromised device, regardless of how securely data is encrypted at rest or in transit:

> "These tools are to protect the content, right? One of the things that we always think is that, if I'm using Signal, I'm secure. No, you are not secure because you're using apps to encrypt content. Anything you use to encrypt content, won't protect you when your device itself it's infected and this is what I always talk about with human rights defenders about devices hygiene."
>
> (Interviewee 9)

However, even if encryption tools for securing online communications or stored data do not have specific capabilities to prevent advanced spyware attacks, their use should of course not be dismissed, respondents said:

> "Using Signal hasn't become completely useless just because of the fact that Pegasus exists, right? But there needs to be a recognition that using digital privacy tools like that and best practices can only get you so far. And when we're talking about the most sophisticated stuff, that isn't as far as it might need to be. But that doesn't make it completely kind of pointless."
>
> (Interviewee 14)

Conclusion

This paper confirms widespread concerns about the dangers and threats that spyware technology poses to journalists and their freedom. Spyware appears to intersect with all dimensions of journalistic safety as expressed by Westlund, Krøvel, and Orgeret (2022). Spyware threatens journalists' safety in terms of a) the digital infrastructure

journalists use to produce news; b) the practices journalists use to report and their epistemologies; and c) the consequences journalists face when they are surveilled and how these affect the production of journalism itself. The power of spyware, visible in all these dimensions, lies primarily in its ability to create uncertainty: uncertainty about the reliability and security of the digital infrastructure of journalism; uncertainty about whether basic practices (such as source protection) can actually be fulfilled and protected; and uncertainty about psychological, political, and social conditions. In terms of infrastructure, the ability of spyware to exploit vulnerabilities in digital tools, potentially turning them into spying devices, calls into question the entire trustworthiness of the online spaces in which and with which journalism is produced. With that trustworthiness in doubt, journalistic practices are also at risk: can journalists effectively protect their sources if the tools they use to communicate could turn against them? Finally, when it comes to the consequences of this situation, spyware can be seen as a crucial factor in making the working conditions of journalists unbearable in psychological, social, and political terms. The fear of being at risk – and the difficulty of verifying the possibility of being a target of spyware – creates extremely difficult psychological conditions for journalists, while the existence of a tool like spyware and its expanding use to target journalists in different geographical areas can be seen as a sign that digital authoritarian practices are becoming increasingly routine (Glasius and Michaelsen 2018).

What worries interviewees most is not what is already known about spyware, but what has yet to be discovered. Overall, journalists seem to be forced to work under a systemic threat that operates stealthily, undermining journalists' safety while leaving no sign of its operation. The aim of surveillance tools such as spyware is maximum invasiveness through "minimum visibility" (Marx 2016: 117), and these dynamics recall the notion of "black box," usually applied to technologies whose technical capabilities and internal politics are barely accountable. While the notion of "black box" is usually applied to algorithms, big data and machine learning tools (Pasquale 2015; Brevini and Pasquale 2020), it can also be applied to spyware and the "techno-fog" (Lyon 2015: 33-349) that surrounds its capabilities. If black boxes are systems whose functions and political-economic characteristics are shrouded in opacity, then spyware is so in several respects: economic, technical, and operational. The impact of this opacity is underlined by the divergent views on the identity of potential targets that emerge from the findings of this paper. The divergent views are the product of the various uncertainties about spyware, ranging from the difficulties of threat assessment to the capabilities of potential attackers, to the technical developments of spyware itself.

Interestingly, respondents discussed spyware and its threats not only in technical terms, but also in socio-technical terms. In this sense, it can be argued that the most dangerous element of spyware is its rhizomatic nature. Spyware appears as the quintessential "surveillant assemblage" (Haggerty and Ericson 2000), whose effectiveness derives from the complex socio-technical ramifications of its interwoven components and the way in which they are obfuscated. This is evident in the technical specifications themselves, but also in how spyware is produced, commercialized and adopted. Furthermore, spyware technology emerges as an assemblage not only through its ability to combine different surveillance elements, technologies, and practices, but

also through its various assemblages of layers of invisibility. This is done through various acts of "blackboxing," which, following Bruno Latour's conceptualization, are processes that "make the joint production of actors and artefacts completely opaque" (Latour 1992: 183). Spyware functions as a "surveillant assemblage" also because of its internal capacity to combine opacity in technological, legal and operational terms. Spyware is created, commercialized, and deployed in the dark, and its success is characterized by invisible access to the data of its targets. Moreover, the success of a spyware attack is represented by the maintenance of this invisibility, making it the quintessential black box technology, again following Latour's idea (Latour 1992: 304) that a black box is made invisible (and thus efficient) by its own operational success.

In addition, these findings are consistent with previous research on journalists and surveillance, particularly in relation to the widespread concern about the security of sources and the general doubts about the available effectiveness of information security practices and encryption. In general, respondents never questioned the usefulness and importance of cryptography. However, when it comes to spyware, even the most secure communications system can do little or nothing to prevent a sophisticated spyware attack. Moreover, according to some of the research discussed in this paper, journalists may even be lulled into a false sense of security about spyware simply because, for example, Signal is used to exchange messages with sources and contacts. What is still needed is a holistic approach to information security that, together with threat assessment, needs to be integrated and accepted into the most common practices of digital journalism in general (Henrichsen, Betz, and Lisosky 2015). In addition, journalists' skills and knowledge of information security and surveillance issues are still limited, which is compounded by the systemic lack of training in this area, as shown by recent research on journalism programs in the US (Henrichsen and Shelton 2022), a situation that is also common in other geographical and cultural areas. Finally, it can't be stressed enough that the most advanced spyware cannot be stopped by any encryption or information security practice. As a recent survey of digital security guides available to journalists online shows (Berdan 2021), journalists have limited and basic access to information on how to protect themselves from spyware, and issues related to malware are not among the most discussed topics in such guides. These concerns shouldn't though lead to fatalistic attitudes. Even if not entirely effective in the context of spyware attacks, encryption strategies and digital hygiene are still pivotal in making such attacks more expensive and complex to be conducted.

On a more meta level, what is the role of journalism in the face of these surveillance threats, if not to be a victim of this situation? Interviewees emphasized that journalists can only find themselves in a position to engage in 'counter-surveillance' (Marx 2003: 384) if they actively contribute to opening the "black box" of spyware through investigation, exposé, and publicity. Instead, by making surveillance itself visible, journalism can find its stronger role in the digital power imbalance that spyware enables and reaffirms. In this sense, the act of investigating and exposing spyware is also a direct action by journalists and technologists to open such a black box. Again, following Latour's terms (Latour 1992: 304), this act of exposure means interrupting the 'success' of the black box by breaking at least some layers of the invisibility of the "surveillant assemblage" that spyware represents. In a broader sense, it can be argued that exposing spyware doesn't just mean investigating a specific

technology and its use, but also contributing to the unmasking of how surveillance works today by actively dismantling some of its components.

Finally, some limitations of this study need to be acknowledged. The article is based on interviews with experts, whose knowledge in the field is stronger than the average journalist. As such, their views on spyware can't be generalized and can't express the general awareness of journalists in Europe, which is expectable to be more limited. More research should be conducted to study and verify the overall preparedness of journalists in face of the threats posed by spyware.

Disclosure Statement

No potential conflict of interest was reported by the author(s).

Funding

This work was funded by The Swiss National Science Foundation (SNSF), Grant/Award Number: P2TIP1_191492.

References

Berdan, Kristin. 2021. "An Evaluation of Online Security Guides for Journalists." Center for Long-term Cybersecurity White Paper Series. https://cltc.berkeley.edu/wp-content/uploads/2021/01/Online_Security_Guides_for_Journalists.pdf.

Biscop, Marjolaine, and David Décary-Hétu. 2022. "Anonymity Technologies in Investigative Journalism: A Tool for Inspiring Trust in Sources." *Journalism Practice* 18 (6): 1420–1441. https://doi.org/10.1080/17512786.2022.2113740

Bradshaw, Paul. 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. https://doi.org/10.1080/21670811.2016.1251329

Braun, Virginia, and Victoria Clarke. 2006. "Using Thematic Analysis in Psychology." *Qualitative Research in Psychology* 3 (2): 77–101. https://www.tandfonline.com/doi/abs/10.1191/1478088706qp063oa. https://doi.org/10.1191/1478088706qp063oa

Brevini, Elisabetta, and Frank Pasquale. 2020. "Revisiting the Black Box Society by Rethinking the Political Economy of Big Data." *Big Data & Society* 7 (2): 205395172093514. https://journals.sagepub.com/doi/10.1177/2053951720935146. https://doi.org/10.1177/2053951720935146

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

Burkart, Patrick, and Tom McCourt. 2017. "The International Political Economy of the Hack: A Closer Look at Markets for Cybersecurity Software." *Popular Communication* 15 (1): 37–54. https://doi.org/10.1080/15405702.2016.1269910

Citizen Lab. 2014. "Hacking Team and the Targeting of Ethiopian Journalists." https://citizenlab.ca/2014/02/hacking-team-targeting-ethiopian-journalists/.

Citizen Lab. 2017. "Reckless Exploit. Mexican Journalists, Lawyers, and a Child Targeted with NSO Spyware." https://citizenlab.ca/2017/06/reckless-exploit-mexico-nso/.

Citizen Lab. 2018. "Hide and Seek. Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries." https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/.

Citizen Lab. 2021. "Forced Entry. NSO Group iMessage Zero-Click Exploit Captured in the Wild." https://citizenlab.ca/2021/09/forcedentry-nso-group-imessage-zero-click-exploit-captured-in-the-wild.

Coleman, Gabriella. 2017. "The Public Interest Hack." Limn, 8. https://limn.it/articles/the-public-interest-hack/.
Committee To Protect Journalists. 2022. "Spyware and Press Freedom." https://cpj.org/spyware/.
Crawford, Kate, and Meredith Whittaker. 2016. "Artificial Intelligence Is Hard to See." *Medium*, September 11. https://medium.com/@katecrawford/artificial-intelligence-is-hard-to-see-a71e74f386db.
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. https://doi.org/10.1080/21670811.2020.1777882
Deibert, J. Ronald. 2013. *Black Code: Surveillance, Privacy, and the Dark Side of the Internet*. New York, NY: McClelland & Stewart/Random House.
Deibert, J. Ronald. 2020. *Reset: Reclaiming the Internet for Civil Society*. Toronto: House of Anansi Press.
Deibert, J. Ronald. 2022. "Subversion Inc: The Age of Private Espionage." *Journal of Democracy* 33 (2): 28–44. https://doi.org/10.1353/jod.2022.0016
Dharampal, Maurice. 2021. "A Theory of Digital Hygiene." Institute of Network Cultures. https://networkcultures.org/blog/2021/05/12/digital-hygiene/.
Di Salvo, Philip. 2021. "We Have to Act like Our Devices Are Already Infected": Investigative Journalists and Internet Surveillance." *Journalism Practice* 16 (9): 1849–1866. https://doi.org/10.1080/17512786.2021.2014346
Di Salvo, Philip. 2022. "Information Security and Journalism: Mapping a Nascent Research Field." *Sociology Compass*. https://doi.org/10.1111/soc4.12961
Farrow, Ronan. 2022. "How Democracies Spy on Their Citizens." *The New Yorker*, April 25. https://www.newyorker.com/magazine/2022/04/25/how-democracies-spy-on-their-citizens.
Forbidden Stories. 2021. "About the Pegasus Project." https://forbiddenstories.org/about-the-pegasus-project/.
Glasius, Marlies, and Marcus Michaelsen. 2018. "Illiberal and Authoritarian Practices in the Digital Sphere." *The International Journal of Communication* 12: 3795–3813. https://ijoc.org/index.php/ijoc/article/view/8899.
González, Rubén Arnoldo, and Frida V. Rodelo. 2020. "Double-Edged Knife: Practices and Perceptions of Technology and Digital Security among Mexican Journalists in Violent Contexts." *Tapuya: Latin American Science, Technology and Society* 3 (1): 22–42. https://doi.org/10.1080/25729861.2020.1746502
Haggerty, D. Kevin and V. Richard Ericson (Eds.) 2016. *The New Politics of Surveillance and Visibility*. Toronto: University of Toronto Press.
Haggerty, D. Kevin, and V. Richard Ericson. 2000. "The Surveillant Assemblage." *The British Journal of Sociology* 51 (4): 605–622. https://doi.org/10.1080/00071310020015280
Harkin, Diarmaid, Adam Molnar, and Erica Vowles. 2020. "The Commodification of Mobile Phone Surveillance: An Analysis of the Consumer Spyware Industry." *Crime, Media, Culture: An International Journal* 16 (1): 33–60. https://doi.org/10.1177/1741659018820562
Harkin, Diarmaid, and Monique Mann. 2023. "Electronic Surveillance and Australian Journalism: Surveillance Normalization and Emergent Norms of Information Security." *Digital Journalism*. Advance online publication. https://doi.org/10.1080/21670811.2023.2220366
Henrichsen, R. Jennifer, and Martin Shelton. 2022. "Boundaries, Barriers, and Champions: Understanding Digital Security Education in US Journalism Programs." *Journalism Studies* 24 (3): 309–328. https://doi.org/10.1080/1461670X.2022.2148267
Henrichsen, R. Jennifer, Michelle Betz, and Joanne M. Lisosky. 2015. "Building Digital Safety for Journalists. A survey of selected issues. UNESCO Series on Internet Freedom." https://www.unesco.org/en/articles/building-digital-safety-journalism-unesco-launches-new-publication.
Henrichsen, R. Jennifer. 2020. "Breaking Through the Ambivalence: Journalistic Responses to Information Security Technologies." *Digital Journalism* 8 (3): 328–346. https://doi.org/10.1080/21670811.2019.1653207
Henrichsen, R. Jennifer. 2022. "Understanding Nascent Newsroom Security and Safety Cultures: The Emergence of the "Security Champion." *Journalism Practice* 16 (9): 1829–1848. https://doi.org/10.1080/17512786.2021.1927802

Information Warfare Monitor. 2009. "Tracking GhostNet: Investigating a Cyber Espionage Network." http://www.infowar-monitor.net/ghostnet.

Jamil, Sadia. 2021. "The Monitored Watchdogs: Journalists' Surveillance and Its Repercussions for Their Professional and Personal Lives in Pakistan." *Journalism Studies* 22 (7): 878–895. https://doi.org/10.1080/1461670X.2021.1904272

Joffe, Helene. 2012. "Thematic Analysis." In *Qualitative Research Methods in Mental Health and Psychotherapy: A Guide for Students and Practitioners*, edited by David Harper, and Andrew R. Thompson. Hoboken: Wiley-Blackwell, 209–223.

Lashmar, Paul. 2016. "No More Sources? The Impact of Snowden's Revelations on Journalists and Their Confidential Sources." *Journalism Practice* 11 (6): 665–688. https://doi.org/10.1080/17512786.2016.1179587

Latour, Bruno. 1992. *Pandora's Hope. Essays on the Reality of Science Studies*. Cambridge, MA: Harvard University Press.

Lyon, David. 2007. *Surveillance Studies: An Overview*. Cambridge, MA: Polity.

Lyon, David. 2015. *Surveillance After Snowden*. Cambridge: Polity.

Marx, T. Gary. 2003. "A Tackle in the Shoe: Neutralizing and Resisting the New Surveillance." *Journal of Social Issues* 59 (2): 369–390. https://doi.org/10.1111/1540-4560.00069

Marx, T. Gary. 2016. *Windows into the Soul. Surveillance and Society in an Age of High Technology*. Chicago, IL: Chicago University Press.

McGregor, E. Susan, and Anne Elizabeth Watkins. 2016. "Security by Obscurity': Journalists' Mental Models of Information Security." *International Symposium on Online Journalism* 6 (1): 33–49.

McGregor, E. Susan, Anne Watkins, Al-Ameen Mahdi Nasrullah, and Kelly Caine. 2017. When the Weakest Link is Strong: Secure Collaboration in the Case of the Panama Papers. 26th Usenix Security Symposium. https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/mcgregor.

McGregor, E. Susan. 2021. *Information Security Essentials. A Guide for Reporters, Editors, and Newsroom Leaders*. New York, NY: Columbia University Press.

Mihalcik, Carrie, and Bree Fowler. 2021. "Apple's Security Fix: Protect Your iPhone from Pegasus Now." *CNet*, September 16. https://www.cnet.com/news/privacy/apples-ios-14-8-security-fix-protect-your-iphone-from-pegasus-now/.

Mills, Anthony. 2019. "Now You See Me–Now You Don't: Journalists' Experiences with Surveillance." *Journalism Practice* 13 (6): 690–707. https://doi.org/10.1080/17512786.2018.1555006

Parikka, Jussi. 2016. *Digital Contagions. A Media Archaeology of Computer Viruses*. New York, NY: Peter Lang.

Pasquale, Frank. 2015. *The Black Box Society. The Secret Algorithms That Control Money and Information*. Cambridge, MA: Harvard University Press.

Pegg, David, Paul Lewis, Michael Safi, and Nina Lakhani. 2021. "FT Editor Among 180 Journalists Identified by Clients of Spyware Firm." *The Guardian*, July 20. https://www.theguardian.com/world/2021/jul/18/ft-editor-roula-khalaf-among-180-journalists-targeted-nso-spyware.

Perlroth, Nicole. 2021. *This Is How They Tell Me the World Ends: The Cyber Weapons Arms Race*. London: Bloomsbury Publishing.

Pew Research Center. 2015. "Investigative Journalists and Digital Security." https://www.pewresearch.org/journalism/2015/02/05/investigative-journalists-and-digital-security/.

Posetti, Julie. 2017. "Protecting Journalism Sources in the Digital Age." UNESCO Publishing. https://en.unesco.org/news/unesco-releases-new-publication-protecting-journalism-sources-digital-age.

R3D. 2022. "Ejército Espía: Fuera de Control." https://ejercitoespia.r3d.mx/.

Stafford, Tom, and Andrew Urbaczewski. 2004. "Spyware: The Ghost in the Machine." *Communications of the Association for Information Systems* 14: 291–306. https://doi.org/10.17705/1CAIS.01415

Tsui, Lokman, and Francis Lee. 2019. "How Journalists Understand the Threats and Opportunities of New Technologies: A Study of Security Mindsets and Its Implications for Press Freedom." *Journalism* 22 (6): 1317–1339. https://doi.org/10.1177/1464884919849418

Watkins, Anne Elizabeth, Nasrullah Al-Ameen, Mahdi, Roesner, Franziska Caine, Kelly, and McGregor, E. Susan 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. https://www.usenix.org/system/files/conference/foci17/foci17-paper-watkins.pdf

Westlund, O., R. Krøvel, and K. S. Orgeret. 2022. "Newsafety: Infrastructures, Practices and Consequences." *Journalism Practice* 16 (9): 1811–1828. https://doi.org/10.1080/17512786.2022.2130818

Woodhams, Samuel. 2021. "Spyware: An Unregulated and Escalating Threat to Independent Media." Center for International Media Assistance. https://www.cima.ned.org/wp-content/uploads/2021/08/CIMA_Spyware-Report_web_150ppi.pdf.

Workneh, T. W. 2022. "From State Repression to Fear of Non-State Actors: Examining Emerging Threats of Journalism Practice in Ethiopia." *Journalism Practice* 16 (9): 1909–1926. https://doi.org/10.1080/17512786.2021.1919176

Zetter, Kim. 2015. *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*. New York, NY: Crown.