Studies in Communication Sciences 20.2 (2020), pp. 243–254

Hybrid professionalism in journalism: Opportunities and risks of hacker sources

Philip Di Salvo*, Università della Svizzera italiana (USI), Institute of Media and Journalism, Switzerland
Colin Porlezza, City, University of London, Department of Journalism, United Kingdom
*Corresponding author: Philip.di.salvo@usi.ch

Abstract
Hackers have a double relevance with regard to the transformation of the journalistic field: first, they have established themselves as journalistic actors, even if their work may sometimes seem unfamiliar. Second, hackers have not only become important sources for information but they are also a topic of public interest in a data-driven society increasingly threatened by surveillance capitalism. This paper critically discusses the role of hackers as news sources by analyzing the "stalkerware" investigation carried out by the online news magazine *Motherboard*. Drawing from field theory and boundary work, the article sheds light on how hackers exert an increasing influence on journalism, its practices, epistemologies, and ethics, resulting in an increasing hybridization of journalism. Journalism has become a dynamic space, in which hackers are not only becoming relevant actors in the journalism field, but they often represent the only sources journalists have to shed light on wrongdoings. Hence, hackers are increasingly defining the conditions under which journalism is carried out, both in terms of its practices as well as in its normative framework.

Keywords
boundary work, field theory, hackers, hacking, hybridity, journalism ethics, news sources

1 Introduction

The past 10 years have seen a progressively more extended presence of hackers in the journalistic field. Hackers have become, on different levels, active journalistic players: they have brought topics and themes on top of journalists' and policy makers' agendas; they have contributed to journalistic practices by providing new tools and technology and, in certain instances, they have become sources providing first-hand source material to investigative reporters (Di Salvo, 2017). News about state-sponsored hacking attacks in the context of political elections, such as those that occurred during the 2016 US Presidential election campaigns, have made the news worldwide and sparked a wide debate around politically motivated hacking and information warfare. At the same time, hacking topics such as cybersecurity, encryption, online privacy, state hacking powers, online surveillance or data breaches and theft are now regularly making the news (Thorsen, 2017). In addition, some data journalists have adopted *de facto* hacking practices for data scraping, data sourcing and have integrated coding as a regular component into their reporting (Usher, 2016). The "Panama Papers" investigation, for instance, has shown the computational element of data-driven reporting at its best (Cabra & Kissane, 2016). Furthermore, hacking-related issues such as information security and the use of encryption software for source protection have also become a topic in particular for investigative journalists, particularly if they work with whistleblowers and other sensible sources (Posetti, 2017). Safer communication tools such as Signal, the Tor Browser, or whistleblowing platforms based on open source software GlobaLeaks and SecureDrop are also progressively becoming routinized in newsrooms (Di Salvo, 2020). And also WikiLeaks, as controversial as it may be as an actor in the media landscape, continues to exert its

https://doi.org/10.24434/j.scoms.2020.02.007

influence on journalism, its practices and epistemologies (Brevini, 2017).

Moreover, some investigations published in the past few years have been based on source materials released by hackers as a result of cyberattacks against institutions or individuals. Gabriella Coleman defines these practices as "public interest hacks" (PIH) (2017a) and has traced their origins back to 2008, when hackers orchestrated the first attack of this kind against the US white supremacist radio host Hal Turner. In Coleman's view, PIHs consist of two separate elements: the "hack" and the "leak" of digital documents. When conducting PIHs, hackers attack servers and communication networks with the aim of extracting otherwise private information with the final purpose of leaking it via different strategies, including dumping or providing it to journalists via encrypted communication channels. Hackers have targeted very different organizations and individuals with PIHs in the past ten years (Coleman, 2017a): politicians or former politicians such as Sarah Palin, Colin Powell and Emmanuel Macron; the Syrian and Peruvian governments; companies such as Sony Pictures and political parties such as the US Democrats and the Turkish AKP, Recep Tayyip Erdoğan's party. In most of these instances, the stolen and leaked materials have been private emails extracted from organizations' servers. Hackers responsible for these PIHs have been affiliated with hacktivist groups such as Anonymous or RevoluSec. Some of them acted on their own, as it is in the case of Phineas Phisher. Others, instead, were under the control of state actors or intelligence agencies, as it is for the infamous Fancy Bear group or the Guccifer 2.0 persona that hacked the US Democratic National Committee in 2016 and released the material using different channels, including WikiLeaks. In some other instances, instead, PIHs have interested private companies operating in the surveillance market, such as the Anglo-German Gamma Group, the Italian Hacking Team, or the Israeli Cellebrite. In these instances, companies have been targeted by hacktivist hackers whose aims have been exposing those firms making their business with non-democratic governments (Citizen Lab, 2013, 2014, 2015; Coleman, 2017a).

This paper will look at a particular case study, the "stalkerware" investigation published by the online magazine *Motherboard*, as an example of how hackers may become journalistic sources. In this particular case, *Motherboard* journalists conducted an investigation into the so-called "stalkerware" software market, based on illegally obtained documents and provided by hackers. Specifically, the documents contained evidence about two firms that produce surveillance software, their distribution and technical details. By asking the question "how are hacker sources changing journalism?", we specifically look at the epistemological and ethical implications such collaborations with hacker sources might entail, particularly when materials obtained from hackers may have been gathered illegally. In particular, we look at whether hackers are accepted as sources within the boundaries of the journalistic field and how this is at the core of the establishment of new professional norms in regards of sourcing.

First, we will offer a description of the specific case discussed in *Motherboard* as it represents the basis of our reflections. We then take a step back and turn to a macro-level perspective in order to analyze how such specific cases are challenging and questioning the boundaries of journalism (Carlson and Lewis, 2015). The use of hacker sources in journalism represents a professional and normative challenge for reporters and journalism and results in a negotiation processes revolving around topics such as hacking, security, journalism ethics and the public interest. In addition, these developments create issues for journalism ethics: while the question of whether and how to use illegally obtained information is all but new, the changing media ecosystem does indeed raise new dilemmas as actors such as WikiLeaks now occupy "the space between publishers, sources and journalists" (Owen, 2016, p. 27) and can, on their own, release information as they see fit or without necessarily involving traditional news

organizations. However, the publication of illegally obtained information can, for instance, entail legal consequences, albeit most often the source – and not the publisher – risks being prosecuted. In addition, there is always the question about the tendency – or (hidden) agenda – of the source. By using one specific case study, this paper offers a theoretical reflection on how hacker sources challenge journalistic boundary maintenance, how they create new moral dilemmas, and how they contribute to the continuous hybridization of journalism and the emergence of new professional norms regarding hackers.

2 The "stalkerware" surveillance market Motherboard investigation

In April 2017, *VICE's* technology channel *Motherboard* published an investigation titled "Inside the 'Stalkerware' Surveillance Market, Where Ordinary People Tap Each Other's Phones," authored by Lorenzo Franceschi-Bicchierai and Joseph Cox (2017), two widely known journalists in the field of technology and information security reporting. The story was based on a cache of hacked documents coming from two US-based companies, Retina-X and FlexiSpy that both specialize in coding and selling "stalkerware", malware software engineered to remotely monitor mobile phones or computers. The peculiarity of the software commercialized by the two companies was their domestic use: in fact, *Motherboard* journalists were able to publish details about a growing market demand from private citizens who use "stalkerware" to monitor their loved ones', employees' or other common people's private communications. As the two journalists wrote in their story, the data for the investigation was provided by two hackers, independent of each other, in part via *Motherboard's* whistleblowing platform, based on the SecureDrop software.[1] The identities of the hackers responsible for the Retina-X and FlexiSpy leak has not been disclosed and only the nickname of one of the two – Leopard Boy – has been revealed. In their reporting, Franceschi-Bicchierai and Cox included some quotes coming from the communication exchanges occurred between them and their sources via online chats. Hackers have explained on the record their motivations and rationales about hacking the two companies and releasing the information to the press (Franceschi-Bicchierai & Cox, 2017). According to Franceschi-Bicchierai and Cox, hackers targeted Retina-X and FlexiSpy to send a message to the industry as a whole. In particular, Leopard Boy, quoted Phineas Fisher, the hacker or group of hackers responsible for the PIHs against surveillance firms Gamma Group and Hacking Team, to explain their motivations: "leaking isn't an end in itself; it's all about the message," said the hacker (Franceschi-Bicchierai & Cox, 2017). For their part, the unnamed hacker added instead more details about what motivated them: "99% of the people being spied on with these things don't deserve to have their lives invaded so much" (Franceschi-Bicchierai & Cox, 2017). In an interview with Leopard Boy, published a few days after the publication of the investigation, Cox and Franceschi-Bicchierai referred to their sources as "hacktivists" (2017).

Joseph Cox has also reflected on the implications of using hacked materials and hackers as sources for journalistic investigation in two different background articles published on *Motherboard* (2016, 2017). In his stories, Cox discusses some of the most pressing ethical and practical issues involved in these reporting scenar-

1 SecureDrop is a technical solution made available by the Freedom of the Press Foundation that enables journalists and news organizations to create an online dropbox whistleblowers and other sources can use to submit documents anonymously and safely over the Internet. When sources approach a SecureDrop on the Internet, their identities are masked by the Tor Browser and other encryption standards to the point that, without any further explicit inquiring, sources' identities are masked even to the receiving journalists. In principle, SecureDrop – as the other available whistleblowing software, GlobaLeaks – is based on the technical approach that WikiLeaks pioneered since 2006.

ios. Interviewing scholar Paul Bradshaw, for instance, Cox discussed the points of contact between whistleblowing-led reporting and reporting on leaks originated from cyberattacks (2016). In the second piece, instead, Cox discussed agenda issues highlighting journalists' need to clarify hackers' motivations for leaking information and consequently take transparency steps to inform readers about the potential controversial origins of the materials used as evidence in the reporting (Franceschi-Bicchierai & Cox, 2017). As Cox (2017) argues, the risk to be primarily avoided from a journalist's perspective is becoming a "puppet" by simply amplifying hackers' agendas or aims for leaking information. Cox's self-reflection about doing journalism with hacker sources offers the possibility to dig into a journalist's reasoning about ethical issues involved in news work and, at the same time, are an occasion to look at how journalists reflects about their roles and how controversial practices, such as reporting on hacks, are negotiated within the journalistic field, and how they contribute to the emergence of new forms of professionalism.

3 Hackers knocking at the door

The participation of hackers into the journalistic field is a sign of how porous the boundaries of the field have become to the influence of new actors who are claiming participation among the journalism realm. In sociology, the notion of "boundary work" has been used to identify and explain instances of different social fields – or fields of knowledge – finding common grounds, developing interconnections and debating proximity and cultural mutual acceptance (Gieryn, 1983). When it comes to journalism, the notion has lately been used as a theoretical framework to discuss the expansion of what is normally conceived and accepted as "journalism" and is thus legitimized and accepted in the journalistic field and within the corpus of professional norms and practices that define journalism as an identifiable activity (Carlson, 2016). Although there is no systematic body of knowledge when it comes to the universally accepted norms, values and routines, formal and on-the-job-training often help defining the profession. Historically, journalists belonging to a legacy news media confirms their acceptance of a specific set of ethical norms and standards, which is essential for offering credible information to the public, but also, in turn, for the audience to believe the journalists' work (Gans, 2003). In particular, as Becker (1967) and Cook (1998) have shown, journalists' legitimacy as servants of the public good stems from their relationship to authoritative and credible sources. At the same time, sources need journalists in order to gain attention, and access to the public (Cook, 1998; Sparrow, 1999).

Leaks and "irregular" journalistic sources, such as WikiLeaks, not only show that the question of credible sources is paramount for the professionalism and the legitimacy of journalism. It also shows that the question of boundaries is relevant when it comes to discourses of acceptance or exclusion from the journalistic field generated by the pressing of newcomers or new practices at the most peripheral areas of it (Wahl-Jorgensen, 2014).

Bourdieu's "Field Theory" is an often-used theoretical background on which discourses about the expansion of the boundaries of journalism and the incorporation of newcomers or the establishment of new practices have been grounded (Bourdieu, 1993, 2005). Following this approach, Eldridge (2014, 2017), for instance, has analyzed how "interlopers" or peripheral players come to terms with the journalistic field and how, despite their irregular traits, their practices can be embraced by more traditional actors, who sit in more established positions within the field. In Eldridge's view (2017), "interlopers" are newcomers to the journalistic field that claim residency in the field despite being non-traditional or irregular players. In *Bourdieuean* terms, fields find their structures and equilibrium when put in relation to the influence expressed by other fields gravitating around them and by demarcating social space in terms of distinction, by

setting boundaries. The journalistic field is among the most exposed to the influence of external factors (Bourdieu, 2005, p. 33), which is why Bourdieu has defined it as a relatively weak field, caught and pressured between politics on the one hand, and economics on the other. In the theoretical debates revolving around journalism as a field, it has traditionally been understood as a heteronomous field and a "site of struggle", where different actors "compete for authority through defining – and contesting – its cultural boundaries" (Carlson and Lewis, 2015, p. 7). Technological shifts, and the way journalism is increasingly impacted by data, algorithms and code (Pavlik, 2016), have also reshaped the relation between journalists and sources, in other words: its internal structure. The integration of "boundary work" and field theory offer a useful lens to analyze ongoing changes in journalism and how these "external changes are 'refracted' at the field's boundaries" (Lowrey, 2018, p. 138). The refraction, and therefore the re-positioning of the boundaries, can be observed in the case of joint ventures between journalists, activists, coders, or hacktivists (Russell, 2016, pp. 68–108; see also Lewis & Usher, 2014).

But technology is not the only terrain on which boundaries get discussed and set: norms, participants and practices are also topics around which "boundary battles" (Russell, 2016, p. 37) are waged along the boundaries of journalism. Following Gieryn's (1983) outline of "boundary work", Carlson and Lewis (2015, pp. 9–12) have produced a framework for analyzing the various forms of "boundary work" in journalism. In their view, "boundary work" in the context of news making can happen on the levels of "participants", "practices" and "professionalism" and follow patterns of "expansion", "expulsion" or "protection of autonomy." The notion is thought to be applied to "who" and "what" is to be considered by journalists as "appropriate" to the field and to establish "journalism" as a distinct community with specialized knowledge (Carlson & Lewis, 2015, pp. 10–11). The typology goes in the direction of defining "boundary work" that is prone to "expand" the limits of what counts as journalism, "expel" those elements that have no legitimate residence in the field or to "protect" journalism from incursions from outside the field that may compromise the autonomy of the field itself. The constant need for journalism to engage in boundary maintenance is due to the fact that journalism does not match the requirements of sociological definitions of professionalism (Eide & Sjøvaag, 2016, p. 4). Independently of the outside pressures applied to the field, the redrawing of the borders of journalism is a constant process that crystallizes those norms, values and myths that ensure stability in the journalism profession. This is also the reason why even traditional professional norms of journalism, such as verification and news gathering have been going through processes of "boundary work" in recent times (Hermida, 2015; Wahl-Jorgensen, 2015). Particularly in the online realm, professional norms are in fact changing as new technologies are adapted into existing newsroom practices and environments (Agarwal & Barthel, 2015). This paper locates the use of hackers as sources within this same contexts of boundaries negotiation, discussing how irregular "interloper" players (Eldridge, 2017) become accepted sources of news, passing through the gates of contemporary journalism. Digitalization has fundamentally changed the way that journalism as a profession relates to its environment: Particularly, the "networked" paradigm of the contemporary news ecosystem has forced journalists to "open the gates for new stakeholders" also in regards of who becomes an accepted source for news (Raeymaeckers, Deprez, De Vuyst, & De Dobbelaer, 2015, pp. 105–107), as it is for hackers, the topic at the core of this paper. This leads to what Eide and Sjøvaag (2016, p. 5) describe as both an ambiguous and a flexible situation, "as journalistic boundary maintenance also implies a challenging and questioning of the borders of the profession". As a consequence, journalism's professionalism is confronted with an interesting paradox at its core

that Anderson (2006) pointed out: while the challenge to strengthen journalism's professionalism through "boundary work" implies a clear demarcation against other professions, journalism also needs to keep its borders open for relevant input, for instance when audience members or experts are asked to contribute to the journalistic practice. Particularly in the current digital environment, van der Haak, Parks and Castells (2012) envision the emergence of a networked journalist, that is "driven by a networked practice dependent on sources, commentaries, and feedback, some of which are constantly accessible online". Such a networked notion of journalism has also led to more dynamic, but also unstable forms of journalism, as journalism startups or collectives have entered the field (Deuze & Witschge, 2020).

Therefore, source materials delivered by hackers might well undergo a similar process of acceptance as it happened with user-generated content. However, hackers remain a controversial news source, as some of them may act on and be motivated by criminal intent, even when they communicate with journalists. These challenges do not only entail questions of "boundary work", but they also force journalists to make the "biases", that is the potentially hidden agenda and motives behind the sources' information, transparent to the audience.

3.1 A hybrid constellation: Between identity reinforcement and openness

The approximation of the journalistic field and the hacking one takes place in a media system whose dynamics and structures are increasingly "hybrid". Chadwick has defined the contemporary "hybrid media system" as built upon "interactions among older and newer media logics" (2017, p. 4) and in his view, media logics can be technologies, genres, norms, behaviors and organizational structures defined in the reflexivity of different fields – intended again in *Bourdieusian* terms – that can relate to each other by process of mutual adaptation or interdependence.

Examples of these hybrid interactions between different – older and newer – logics have been visible on various levels, especially with the adoption of digital technology for reporting. For Chadwick (2017, pp. 103–129), WikiLeaks – a contested journalistic institution with profound hacker roots and practices – has represented one of the most powerful examples of how players embodying stances from different fields may position themselves between sources and publishers, and therefore along the boundaries of journalism, constantly acting as bridges between the two sides of the spectrum. The "boundary work" between hacker sources and journalists in the Retina-X and FlexiSpy investigation bears more nuanced interpretations. In fact, although there is no doubt that conducting cyberattacks against companies' servers is an illegal act, the agenda and motivations of the hackers who shared the hacked information with the journalists clearly had a political and hacktivist nature of the kind which would fit under the "data activism" label (Milan and van der Velden, 2016). Data activism, in this sense, can be understood as a social practice that is deeply rooted in technology that also takes a "critical view towards datafication" (Gutiérrez, 2018, p. 1). The aspect of social change is at the heart of such proactive data activism (Milan & Gutiérrez, 2015), particularly if one takes into account that huge data vaults are controlled by private organizations and governments without being transparent, accessible or accountable – which led Caron (2016) to define this the "era of the leak". Albeit not being journalistic actors themselves, hackers such as the ones in the "stalkerware" investigation, can nevertheless influence the way that journalists operate in these circumstances and contribute to an "emerging liminal press", here intended as a set of field level relationships among actors who can define the conditions under which news is created and circulates despite not necessarily self-identify as journalists (Ananny & Crawford, 2015, p. 193). For these actors are driven by the emergent networks determined by a more dynamic ecosystem of

information sharing (Owen, 2016, p. 33), they produce new journalism practices that extend themselves between different identities, ideologies and assumptions about the intersection of news and public life (Ananny & Crawford, 2015). As a consequence, however, they also produce uncertainty within the profession, not least from an ethical perspective.

3.2 The ethical challenges of hacking

Contemporary forms of investigative reporting, such as those that rely on the use of technology such as whistleblowing platforms, or that make use of leaks, have already shown their impact on the "boundary work" regarding the practices of journalism. However, they also raise new issues in relation to journalism ethics. While the question of how and whether to use illegally obtained information is not a novelty in journalism, it is the changed media ecosystem that instills the problem with new aspects. Given the existence of organizations such as WikiLeaks, that operate in a border space among different journalistic actors, access to information is no longer limited to journalists and sources. And sources such as hackers have now other means to publish information as the information spaces are no longer exclusively controlled by traditional media institutions (Owen, 2016, p. 31). This brings us to the main ethical question: how can journalists make sure to preserve their obligation to truth, accuracy and facticity? And how can they avoid becoming puppets, whose strings are pulled by (hidden) political actors when publishing illegally obtained materials (Cox, 2017)?

When it comes to collaborative investigations between whistleblowers and journalists, previous research has shown that the performance of accountability in such whistleblowing-induced investigations may be "shared" between sources and journalists (Porlezza & Di Salvo, 2019). However, in the case where journalists are offered illegally obtained materials from hackers, the moral quandaries may be different, especially when players involved are particularly controversial or do not follow established journalistic ethical norms. Additionally, the problem of accuracy and facticity is enhanced by the fact that, nowadays, leaking has not only become easy as many news outlets have developed their own platforms, but it has become part of the daily news production:

> Like the appetite for leaks, the risks have also grown, and now have to be weighed at a faster pace than ever. Where leaks were once a first step in the long, deliberative process of investigative journalism, they're now part of a hyperactive daily news cycle. (Marcus, 2017)

Additionally, as journalists are working in a digital environment, most of their activities are somehow traced and tracked, meaning that

> all too easy to inadvertently reveal the direction of an ongoing investigation. Moreover, because leaks are now often larger than any one journalist – or journalistic organization – can typically handle, they present unique collaboration and publication challenges, all of which must be carefully engineered to balance efficacy, transparency, and privacy. (McGregor & Brennan, 2019)

However, the way that (illegal) information is obtained does not change the journalistic responsibilities with regard to the usual verifications to apply to newly gained material or to source protection. What changes, though, is the handling of the information, not only because digital datasets can involve incredibly large amounts of data and metadata and keeping them safe and secure can be challenging, but also because journalists might get in touch with highly sensitive information that represent an issue for the balancing of privacy and transparency. Additionally, data often misses contextual information, which makes it hard to understand the potential impact of the investigations. There are thus also the risks of selectivity and hermeticism, if the overall significance of a leak is unknown (Christofoletti, 2016).

In addition, the real intentions of hackers can remain unknown to the journalists. Even if journalists are able to discuss the motives with the hackers, as it was the case in the "stalkerware" example, the real intentions can remain dubious, which is why this has to be one of the core questions of journalists when it comes to such collaborations (Gourarie, 2015), especially when hacker sources do not present an explicit political or hacktivist agenda or public interest motivations. As Cox's (2016) own meta-journalistic discourse shows, this is a central issue since "hacks vary greatly in quality, depth and importance". As hackers, who may have a different ethical and cultural framework, are increasingly operating within the boundaries of journalism, there will be a process of mutual adaptation and interdependence when it comes to journalistic norms.

4 Conclusion

Journalism has become a dynamic space. In this changing media ecosystem, hackers are becoming relevant actors in the journalism field, not only because they can actually cover journalistic roles, but also because they often represent the only sources journalists have to shed light on wrongdoings that threaten the public interest (Bok, 2003). When it comes to topics related to surveillance, cybercrime or the secretive market of snooping technology, hackers – together with whistleblowers – may be the only sourcing option for journalists. Moreover, in recent years, hackers have also expanded the scope of their activist and hacktivist involvement, becoming more and more actively engaged as "public participants in our daily geopolitical goings-on" (Coleman, 2017b, p. 91) finding in journalism a terrain for cooperation and influence. In asking the question "how are hacker sources changing journalism?", the discussed example permits to reach some conclusions: first of all, it shows that hackers are contributing to the ongoing "boundary work" in journalism. Most importantly, hackers are increasingly defining the conditions under which journalism is carried out. By doing so, hackers are influencing the journalistic practice as well as its normative framework, pushing journalists to come to terms with working in growingly complex and sometimes controversial grounds. Albeit some of the ethical considerations are certainly not new (verification, accuracy, truth), other issues have become paramount: questions of privacy, transparency, security, and attribution. This is a direct consequence of the wider change in the journalistic field that can be traced back to a networked organization of newswork and to the consequent expansion of the boundaries of the journalistic field. Whether this networked orientation of journalism has been originated by economic reasons (by pooling together human, financial and technological resources, or even through integration and convergence strategies in news organizations due to economic shortcomings), or by cultural changes due to new actors entering the field of journalism (for instance in the area of data and interactive journalism figures such as computer engineers, data scientists, design specialists, activists or – well – hackers) is hard to tell. We are inclined to believe the latter, as other studies have shown (Agarwal & Barthel, 2015).

The "boundary work" concept is useful to understand the current media landscape and the technological change and dependency that it has brought along. The *Motherboard* "stalkerware" investigation offers a clear example of "boundary work" at play in the context of sourcing. Applying again Carlson and Lewis' (2015, pp. 9–12) framework, the use of hackers as sources can be seen from two different perspectives: a) as a sing of "expansion" of the boundaries of journalism, as "interloper" (Eldridge, 2017) actors such as hackers become accepted as sources within the journalistic field and b) as a sign of "protection of autonomy", since – as Cox self-reflection articles show (2016, 2017) – journalists respond to this adoption with strategies that re-enforce their professional roles and independence. While we must avoid falling for any form of technological determinism, it is nevertheless useful to remind ourselves that contemporary

journalism needs a more complex understanding of the role and impact of journalists than what orthodox perspectives of professional journalism may be able to offer. The example analyzed in this article shows how "boundary work" in journalism can also be related to core elements of the profession, including sourcing strategies and actors who can be accepted as sources of information. Hackers, in this sense, contribute to the continuous evolution of the field. As Deuze and Witschge (2020, pp. 125–126) state: "there is not just one journalism, there are many forms, and it is forever changing, forever becoming: each new form and practice of journalism adds to what we consider to be journalism." Yet, despite the growing presence of hackers in the public sphere, we should also not forget that hacker-sourced investigations are still a highly specialized and rare area of reporting: journalists working in this field usually have a strong background in information security, coding and may be considered as "hacker-journalists" (Parasie, 2011) themselves. In other words: these hacker-journalists may have developed their own professional identity in a hybrid environment. In this sense, they could also be considered as "pioneer journalists" (Hepp & Loosen, 2019), for they act as "intermediaries" (Bourdieu, 2010) between the journalistic field and what hackers have to offer from the outside, pushing for the normalization of the practice within the journalistic field. In the sense, this article showed exactly how journalism is changing, and how new actors are becoming part of its field within the boundaries of the profession. But it also shows, that this new hybridity of journalism does not come without any challenges: they have to be tackled both by the profession with regard to possible standards and principles of self-regulation, and they have to be negotiated within news organizations – start-ups or legacy media alike – by journalists and media managers, as they try to make sense of these changes.

As with other works based on specific case studies, this paper is not free from limitations, starting from being based on a single – yet almost unique in its kind – case study. The case was limited to one particular investigation, in one particular online news outlet, in which the role of hackers as news sources played a crucial role. Albeit single case studies can offer a nuanced and context-rich insight into a particular phenomenon, they remain subject to the limitation of generalizability. However, even if this is a valid criticism, it was never our intention to strive for the generalization of our findings, but on the contrary, for their particularisation by a strategic selection of the case, which allows for an exploratory and analytical deep dive. Therefore, we feel confident in the findings and their contribution to a specific field of research that still lacks a thorough investigation. We therefore suggest that future research should include further empirical investigations to detail what new types of norms emerge in the newsrooms, or what kind of norms are adapted by the inclusion of hacker sources. Additionally, given that hacking is a global phenomenon, future scholarship should also consider either case studies from other countries, or even comparative analyses of how hacker sources are experienced in different newsrooms.

References

Agarwal, S. & Barthel, M. (2015). The friendly barbarians: Professional norms and work routines of online journalists in the United States. *Journalism, 16*(3), 376–391.

Ananny, M. & Crawford, K. (2015). A liminal press: Situating news app designers within a field of networked news production. *Digital Journalism, 3*(2), 192–208.

Becker, H. S. (1967). Whose side are we on? *Social Problems, 14*(3), 239–247.

Bok, S. (2003). The morality of whistle-blowing. In M. D. Ermann & M. S. Schauf (Eds.), *Computers, ethics and society* (pp. 42–47). Oxford: Oxford University Press.

Bourdieu, P. (1993). *The field of cultural production.* New York: Columbia University Press.

Bourdieu, P. (2005). The political field, the social science field, and the journalistic Field. In R. Benson & E. Neveu (Eds.),

Bourdieu and the journalistic field (pp. 29–47). Cambridge: Polity.

Bourdieu, P. (2010). *Distinction*. London: Routledge.

Brevini, B. (2017). WikiLeaks: Between disclosure and whistle-blowing in digital times. *Sociological Compass, 11*(3), 1–11. https://doi.org/10.1111/soc4.12457.

Cabra, M. & Kissane, E. (2016, May 10). The people and the technology behind the Panama Papers. *Global Investigative Journalism Network (GIJN)*. Retrieved from https://gijn.org/2016/05/10/the-people-and-the-technology-behind-the-panama-papers/.

Carlson, M. (2016). Metajournalistic discourse and the meanings of journalism: Definitional control, boundary work, and legitimation. *Communication Theory*, *26*(4), 349–368.

Carlson, M., & Lewis, S. C. (Eds.). (2015). *Boundaries of journalism: Professionalism, practices and participation*. London: Routledge.

Caron, G. (2016, September 8). From Liechtenstein to Panama: The era of the leak. *The Huffington Post*. Retrieved from https://www.huffingtonpost.ca/guy-caron/era-of-the-leak_b_11892222.html.

Chadwick, A. (2017). *The hybrid media system: Politics and power* (2nd ed.). Oxford: Oxford University Press.

Christofoletti, R. (2016). Ethical risks, informers, whistleblowers, leaks and clamor for transparency. *Brazilian Journalism Research, 12*(2), 54–73.

Citizen Lab. (2013, March 13). You only click twice. FinFisher's global proliferation. *The Citizen Lab*. Retrieved from https://citizenlab.ca/2013/03/you-only-click-twice-finfishers-global-proliferation-2/.

Citizen Lab. (2014, June 24). Hacking team malware targeting shia community in Saudi Arabia. *The Citizen Lab*. Retrieved from https://citizenlab.ca/2014/06/hacking-team-malware-targeting-shia-community-saudi-arabia/.

Citizen Lab. (2015, March 9). Hacking team reloaded? US-based Ethiopian journalists again targeted with spyware. *The Citizen Lab*. Retrieved from https://citizenlab.ca/2015/03/hacking-team-reloaded-us-based-ethiopian-journalists-targeted-spyware/.

Coleman, G. (2017a). The public interest hack. *Limn*, 8, 18–23.

Coleman, G. (2017b). From internet farming to weapons of the geek. *Current Anthropology*, *58*, 91–102.

Cook, T. E. (1998). *Governing with the news: The news media as a political institution*. Chicago: University of Chicago Press.

Cox, J. (2016, April 7). Journalists should not be afraid of using hacked data. *Motherboard*. Retrieved from https://www.vice.com/en_us/article/qkjkg3/journalists-should-not-be-afraid-of-using-hacked-data.

Cox, J. (2017, May 5). How to report on a hack without becoming a puppet. *Motherboard*. Retrieved from https://www.vice.com/en_us/article/bmwzb4/how-to-report-on-a-hack-without-becoming-a-puppet.

Cox, J. & Franceschi-Bicchierai, L. (2017, April 19). "I'm going to burn them to the ground": Hackers explain why they hit the stalkerware market. *Motherboard*. Retrieved from https://www.vice.com/en_us/article/vvabv3/hackers-why-they-hit-stalkerware-flexispy-retina-x.

Deuze, M. & Witschge, T. (2020). *Beyond journalism*. Cambridge: Polity Press.

Di Salvo, P. (2017). Hacking/Journalism. *Limn*, *8*, 36–39.

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

Eide, M. & Sjøvaag, H. (2016). Journalism as an institution. In M. Eide, H. Sjøvaag & L. O. Larsen (Eds.), *Journalism re-examined* (pp. 3–14). Chicago: Intellect.

Eldridge, S. A. (2014). Boundary maintenance and interloper media reaction: Differentiating between journalism's discursive enforcement processes. *Journalism Studies, 15*(1), 1–16.

Eldridge, S. A. (2017). *Online journalism from the periphery: Interloper media and the journalistic field*. London: Routledge.

Franceschi-Bicchierai, L. & Cox, J. (2017, April 18). Inside the "stalkerware" surveillance market, where ordinary people tap each other's phones. *Motherboard*. Retrieved from https://www.vice.com/en_us/article/53vm7n/inside-stalker-

ware-surveillance-market-flexispy-retina-x.

Gans, H. (2003). *Democracy and the news*. Oxford: Oxford University Press.

Gieryn, T. F. (1983). Boundary-work and the demarcation of science from non-science: Strains and interests in professional ideologies of scientists. *American Sociological Review, 48*(6), 781–795.

Gourarie, C. (2015, August 21). Is it ethical to write about hacked Ashley Madison users? *Columbia Journalism Review*. Retrieved from https://www.cjr.org/criticism/ashley_madison_hack_reporting.php.

Gutierrez, M. (2018). *Data activism and social change*. Cham: Palgrave.

Hepp, A. & Loosen, W. (2019). Pioneer journalism: Conceptualizing the role of pioneer journalists and pioneer communities in the organizational refiguration of journalism. *Journalism*. Advance online publication. https://doi.org/10.1177/1464884919829277.

Hermida, A. (2015). Nothing but the truth. Redrafting the journalistic boundary of verification. In M. Carlson & S. C. Lewis (Eds.), *Boundaries of journalism: Professionalism, practices and participation* (pp. 22–36). London: Routledge.

Hermida, A. & Lynn Young, M. (2019). *Data journalism and the regeneration of news*. London: Routledge.

Johnston, L. (2016). Social news = journalism evolution? How the integration of UGC into newswork helps and hinders the role of the journalist. *Digital Journalism, 4*(7), 899–909.

Lewis, S. C. & Usher, N. (2014) Code, collaboration, and the future of journalism: A case study of the Hacks/Hackers global network. *Digital Journalism, 2*(3), 383–393.

Lowrey, W. (2018). Journalism as institution. In T. P. Vos (Ed.), *Journalism* (pp. 125–148). Berlin: De Gruyter.

Marcus, J. (2017). The ethics of leaks. *Nieman Reports*. Retrieved from https://niemanreports.org/articles/the-ethics-of-leaks/.

McGregor, S. & Brennan, A. (2019). Privacy and data leaks. *Data journalism handbook*. Retrieved from https://datajournalism.com/read/longreads/privacy-and-data-leaks.

Milan, S. & Gutiérrez, M. (2015). Citizens' media meets big data: The emergence of data activism. *Mediaciones, 14*, 120–133.

Milan, S. & van der Velden, L. (2016). The alternative epistemologies of data activism. *Digital Culture & Society, 2*(2), 57–74.

Owen, T. (2016). Global media power. In T. Witschge, C. W. Anderson, D. Domingo & A. Hermida (Eds.), *The Sage handbook of digital journalism* (pp. 25–34). London: Sage.

Parasie, S. (2011, October 14). 'Hacker' journalism – A new utopia for the press? *Books & Ideas*, Retrieved from https://booksandideas.net/Hacker-Journalism-A-New-Utopia-for.html.

Pavlik, J. V. (2016). Data, algorithms, and code. Implications for journalism practice in the digital age. In B. Franklin & S. Eldridge II (Eds.), *The Routledge companion to digital journalism studies* (pp. 265–273). London: Routledge.

Porlezza, C. & Di Salvo, P. (2019). Ensuring accountability and transparency in networked journalism. In T. Eberwein, S. Fengler & M. Karmasin (Eds.), *Media accountability in the era of post-truth politics* (pp. 212–226). London: Routledge.

Posetti, J. (2017). *Protecting journalism sources in the digital age*. Unesco Publishing. Retrieved from https://unesdoc.unesco.org/ark:/48223/pf0000248054.

Raeymaeckers, K., Deprez, A., De Vuyst, S. & De Dobbelaer, R. (2015). The journalist as a jack of all trades: Safeguarding the gates in a digitized news ecology. In Vos, T. & Heinderyckx, F. (Eds.), *Gatekeeping in transition* (pp. 104–120). London: Routledge.

Russell, A. (2016). *Journalism as activism: Recoding media power*. Cham: Polity.

Sparrow, B. H. (1999). *Uncertain guardians: The news media as a political institution*. Baltimore: Johns Hopkins University Press.

Thorsen, E. (2017). Cryptic journalism: News reporting of encryption. *Digital Journalism, 5*(3), 299–317.

Usher, N. (2016). *Interactive journalism: Hackers, data, and code*. Champaign: University of Illinois Press.

Van der Haak, B., Parks, M. & Castells, M. (2012). The future of journalism: Net-

worked journalism. *International Journal of Communication, 6*, 2923–2932.

Wahl-Jorgensen, K. (2014). Is WikiLeaks challenging the paradigm of journalism? Boundary work and beyond. *International Journal of Communication, 8*, 2581–2592.

Wahl-Jorgensen, K. (2015). Resisting epistemologies of user-generated content? Cooptation, segregation and the boundaries of journalism. In M. Carlson & S. C. Lewis (Eds.), *Boundaries of journalism: Professionalism, practices and participation* (pp. 169–185). London: Routledge.