



Hacked, Leaked, Reported: Journalistic Practices and the Logics of Disclosure in a Turbulent Cyber Landscape

Philip Di Salvo

To cite this article: Philip Di Salvo (28 Jul 2026): Hacked, Leaked, Reported: Journalistic Practices and the Logics of Disclosure in a Turbulent Cyber Landscape, Journalism Practice, DOI: [10.1080/17512786.2026.2708144](https://doi.org/10.1080/17512786.2026.2708144)

To link to this article: <https://doi.org/10.1080/17512786.2026.2708144>



© 2026 The Author(s). Published by Informa UK Limited, trading as Taylor & Francis Group



Published online: 28 Jul 2026.



Submit your article to this journal [↗](#)



Article views: 530



View related articles [↗](#)



View Crossmark data [↗](#)

Hacked, Leaked, Reported: Journalistic Practices and the Logics of Disclosure in a Turbulent Cyber Landscape

Philip Di Salvo

Institute for Media and Communications Management (MCM), University of St. Gallen, St. Gallen, Switzerland

ABSTRACT

Journalists increasingly report on data that surface through direct hacks, *hack-and-leak* operations, cybercrime leaks, and large-scale data dumps. In this environment, the motives and ethical boundaries of hacker sources are often unclear, blurring the lines between crime, espionage and hacktivism. This ambiguity creates crucial editorial and ethical challenges, especially when journalists receive data obtained through cyberattacks and offered for its political or informational value. More complex than more traditional investigations involving whistleblowers or other controversial but familiar source relationships, these reporting scenarios define a new reality for journalists covering cyber-related issues and, increasingly, other topics. This paper examines how journalists navigate these dilemmas by analyzing their editorial choices, investigative techniques, and verification processes. It draws on qualitative interviews with expert journalists in the US, Europe, and the UK who routinely work with hacked materials and interact with hacker sources across beats such as technology, cybersecurity, conflict, and politics. The article aims to illuminate how journalists manage relationships with hacker sources, assess the credibility and origin of digital leaks, and adopt transparency measures when reporting on them. Overall, the paper highlights emerging but increasingly central practices shaping journalism in an era where reporting on and from cyberspace and through cyber-derived sources has become essential.

KEYWORDS

Journalism; Hacking; Investigative journalism; Computational journalism; Journalism sources; Data journalism

Introduction

Increasingly, journalistic stories are based on materials and data coming from hackers, including leaked databases and internal documents, emails, and other potentially newsworthy sources (Di Salvo 2020; Lee 2024). Cases span a wide range of beats, from cybercrime, corruption, and international affairs to cybersecurity, technology reporting, and political journalism. Notable examples include the 2016 leaks of Hillary Clinton campaign emails linked to hackers operating within the Russian intelligence (Marmura 2018; Shapiro

CONTACT Philip Di Salvo  philip.disalvo@unisg.ch

This article has been corrected with minor changes. These changes do not impact the academic content of the article.

© 2026 The Author(s). Published by Informa UK Limited, trading as Taylor & Francis Group

This is an Open Access article distributed under the terms of the Creative Commons Attribution License (<http://creativecommons.org/licenses/by/4.0/>), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited. The terms on which this article has been published allow the posting of the Accepted Manuscript in a repository by the author(s) or with their consent.

2023, 224–237), the hacktivist collective Phineas Fisher’s operations targeting European surveillance companies (Maynard and McLaughlin 2020), and journalistic investigations prompted by the Russian invasion of Ukraine, based on hacked documents obtained by actors of diverse affiliations (Lin 2022). Reporting on hacked materials has also become integral to open source investigations (OSINV), at times providing additional context and verification for complex stories (Khan et al. 2025). Overall, the use of hacked data has grown in volume, complexity, and geographical scope, ranging from singular high-profile leaks to diverse datasets obtained from hacktivists and ransomware groups (Philp 2023).

During the 2010s, the distance between hackers and journalists decreased through mutual engagement: hacking became not only a topic of coverage (Meissner, Wilke, and Puikytė 2025) but also an adjacent field enabling boundary work around technologies, infrastructures, and investigative methods (Di Salvo 2020; Usher 2018). Later, the rise and institutionalization of data journalism has further encouraged newsrooms to integrate data of various origins into reporting and investigative routines (Schaetz, Lischka, and Laugwitz 2025). Leak-based practices, beginning with WikiLeaks¹ and continuing through subsequent operations, also established hacking as a key source of journalistic information (Di Salvo 2024; Hosaka 2025). In its diverse forms, from cybercrime and state-sponsored operations to hacktivism, hacking has become a central phenomenon of the datafied society, particularly because its public-facing nature shapes discourse, media coverage, and political debate (Coleman 2017b; Dutton 2023, 139–156).

Within this framework, this paper examines how journalists relying on hacker sources understand and conceptualize this practice. It explores the reporting dilemmas arising from engagement with hackers and the often controversial data they provide, as well as the routines shaping such reporting. By focusing on “pioneering journalists” (Hepp and Loosen 2021), the paper highlights distinctive features of an emergent reporting practice situated at the intersection of investigative journalism, leak-based reporting, technology journalism, and computational methods. Although this type of reporting remains a niche, it certainly offers insights into the entanglement between journalism, hacking, and processes of datafication. In an era in which the cyber and hackable dimensions of society intersect with issues such as warfare and political upheaval (Whyte 2020), how journalists integrate these disruptions while navigating ethical, legal, and epistemic complexities reveals a reflexive dynamic at the heart of contemporary journalism: rather than observing the datafied society from outside, they increasingly rely on phenomena such as hacking to make sense of the systems they inhabit (Porlezza 2018).

Crossroads of Hackers and Journalists

Over the past decade, the convergence between hackers and journalists has reshaped sourcing norms and the ethical boundary work defining professional journalism (Carlson 2016; Carlson and Lewis 2015). This convergence occurs on two levels. First, at

¹The WikiLeaks releases during this period were among the most impactful, inaugurating an era in which digital leaks came to occupy a central role in journalism. It should be emphasized that, although WikiLeaks has at times published data obtained from hackers - such as Anonymous (Coleman 2015) - and despite the organization’s hacker roots, it has consistently acted only as a publisher of such information, sometimes in collaboration with other news outlets and sometimes independently (Di Salvo 2020).

the level of logics (Altheide 2015), journalism increasingly adopts and responds to the cultural, political, and epistemic logics associated with hacking, for example valuing transparency through leaks, embracing an “exposure” ethos, and engaging with adversarial information flows shaped by *hack-and-leak* operations sometimes provided by organizations with explicit hacking connotations² (Ruohonen, Hjerpe, and Von Zastrow 2024). Second, at the level of practices and skills, journalists have incorporated techniques long associated with hacking, such as secure communication, encryption (Di Salvo 2020; McGregor 2021), advanced verification of digital traces, and data forensics, into investigative routines (Gates 2020).

Early cultural histories of hacking established the heterogeneous moral logics and political imaginaries of hacker communities, showing that many hackers see their activities as forms of political speech, civic intervention, and hacktivism (Coleman 2015). Different hacker typologies have positioned themselves in media advocacy, policy-making, political tool building, and certainly civil disobedience (Coleman 2017a; Jordan 2017), thus reinforcing their public presence. Hackers and journalists have thus developed “trading zones” of mutual influence (Di Salvo 2020; Lewis and Usher 2016), in which hackers find attentive recipients for their public-oriented actions and journalists gain sources, mostly through leaks. This convergence has been reinforced by the growing centrality of information security (infosec) within contemporary reporting. While other computational skills, such as data journalism and algorithmic accountability reporting, have entered journalism (Lewis and Usher 2016), infosec retains the strongest “hacker” connotations, as its use is central to hacker identities and cultures (Ross 1990; Westlund, Krøvel, and Orgeret 2024).

The literature treats journalist–hacker collaboration as a hybrid practice that has produced real investigative capabilities for public-interest reporting while outpacing the ethical norms, technical competencies, and institutional safeguards needed to govern it (Crete-Nishihata et al. 2020; Usher 2018). This dynamic is evident when journalists rely on hacked materials as source evidence, especially in *hack-and-leak* contexts where hackers disclose data obtained through cyberattacks for its inherent public or political value (Coleman 2017b). Similarly, Di Salvo (2024) shows how these data breaches, compared to insider whistleblowing, complicate journalistic routines of sourcing, verification, and narrative construction, adding hackers as potential journalistic sources.

The scholarly attention devoted to journalist-hacker encounters has been concentrated predominantly in North America and Europe, but evidence of analogous dynamics is emerging from the Global South. For instance, Träsel (2018) documents how the Brazilian data journalism unit *Estadão Dados* developed a professional ethos inflected by hacker values, while Araujo and Belim (2024) show how journalists at *Folha de S.Paulo* partnered with *The Intercept Brazil* to publish hacker-obtained material. Barr and Liemann Escobar (2023) extend this picture further, illustrating how journalists and researchers mediated access to data from hacktivist group Guacamaya’s leaks across nine Latin American states, and Scott (2024) shows collaborative investigative networks

²The pioneering organization in this space is again WikiLeaks, particularly in its use of encryption to advance journalistic principles such as source protection and whistleblower-supporting practices (Di Salvo 2020). More recent examples include Distributed Denial of Secrets (DDoSecrets), which specializes in publishing leaked data and information originating from *hack-and-leak* operations (Di Salvo 2024). While operating independently most of the time, the organization has also collaborated with established news outlets (see Philp 2023).

operating across continents. These cases suggest that trading zones between hackers and journalists are being actively constituted also in the Global South, often under conditions of greater political precarity and weaker press protections, which may render the ethical and epistemic tensions inherent to such collaborations still more acute.

All these dynamics generate a profound epistemic and ethical tension at the core of contemporary journalism: while hacked leaks can provide access to information that would otherwise remain permanently concealed, they simultaneously destabilize the boundaries between legality and illegality, transparency and opacity, and professional journalism, activism, and cybercrime, boundaries that the field has long relied upon to define and legitimate itself.

Between Newsworthiness and Harm: The Ethics of Hacker Sourcing

The use of hacker sources in journalism can be positioned within the broader expansion of potential sources that journalists can rely on in the context of digi- and datafication (Heinrich and Spyridou 2025). Although the journalist–hacker sourcing relationship introduces novel technical, ethical, and security challenges, its dynamics can still be analyzed through classic scholarship on journalist–source interactions (see, for instance, the overviews by Berkowitz 2019; Carlson 2009) and ethics in journalism. From the sourcing perspective, for instance, Sigal (1973, 111–115) classically identified notoriously emphasized the importance of “informal” channels in news production, an analytical space into which hacker-sources also fit. More recently, Wheatley (2020, 287) describes leaks as a “non-routine” channel of news production, offering news organizations prestige, exclusivity, and agenda-setting opportunities, but also requiring stronger verification strategies, which can be resource-intensive and carry severe legal risks, elements that are even more controversial when sources are hackers and not insider whistleblowers.

From the perspective of ethics in journalism, hacker sources present distinct challenges, particularly given the illegal origins of the materials and the potentially criminal acts involved in obtaining them (Vanacker 2021). The spread of hacked data online in different digital spaces, as it will be discussed, further complicates reporting. As Sauter (2017) observes, leaked or hacked data can carry an “illicit aura” that shapes how information is perceived, circulated and also analyzed, also frequently allowing online non-expert communities to interpret material before journalists can provide context. Scholars have emphasized that *hack-and-leak* scenarios differ from traditional whistleblowing, requiring distinct considerations in handling and verification (Zittrain 2016). Nevertheless, as Vanacker (2021) notes in discussing hacked data, journalists often prioritize the newsworthiness and informational value of materials over the motives of the source, as also media-ethics textbooks do (Duffy and Freeman 2011, quoted in Vanacker 2021).

Ward (2015) argues that the digital transformation of journalism has rendered traditional ethical codes inadequate for some digital reporting contexts. This is visible, for instance, with decisions about publishing sensitive materials – such as hacked data – that require a situated assessment of democratic value. This matters acutely in the context of hacker sourcing because, unlike conventional whistleblowers whose disclosures typically arise from insider knowledge of specific wrongdoing, hacker sources operate across a broad spectrum of motivations—political, ideological, criminal, or connected to influence operations—that directly affect how their materials should be

handled and contextualized (Vanacker 2021; Zittrain 2016). Large hacked datasets compound this further by potentially containing private information about individuals who are not newsworthy, and whose exposure may carry serious personal consequences, as emerged in open source investigations (Van Der Woude, Dodds, and Torres 2025), a problem made worse by the fact that self-regulatory frameworks governing data-driven journalism have been consistently slow to adapt to these challenges, leaving journalists in largely uncharted normative territory (Porlezza 2024).

Once journalists engage with hacked data or hacker sources, a negotiation process unfolds, shaped by the unique risks and uncertainties of illicit data (Ericson, Baranek, and Chan 1989), and aimed at verification, ethical analysis and newsworthiness establishment. Waters (2020), in a study of how journalists navigate trust relationships with whistleblowers, suggests that this negotiation depends on an internalized but consistent ethical reasoning that operates outside formal codes, while still mirroring those journalistic values. This resonates with the virtue-ethics tradition: Karen Sanders, for instance, argues that journalism ethics cannot be reduced to rule-application because the profession sometimes confronts dilemmas that are novel and resistant to resolution by any pre-established code, if not “irresolvable” (Sanders, 2003, 35–37). These situations require instead *phronesis* - or practical wisdom - understood as the capacity to identify all factors at play in a situation and judge how to act in response to them (Sanders 2003, 35–38; 71–72). Steel, Firmstone, et al. (2025) echo this: in interviews with twenty-seven journalists across five European countries, they find that ethics codes, still central, sometimes operate “in the background,” with journalists referring to internalized values and judgment emerging from experience when working under pressures brought by declining trust (Steel, Firmstone, et al. 2025, 2957 - 2962). For hacked-data journalism, this means that even where the public interest justification seems robust and the material is rigorously verified, the ethical ledger is not automatically balanced, since publication may still cause harm (for this debate in the context of WikiLeaks, see Elliott 2013).

Viewed through this lens, the journalist–hacker relationship appears both new and familiar: new in its infrastructures, risks, and opacity, yet still rooted in the strategic negotiations and asymmetrical information dynamics that have long defined reporter–source relations and what becomes news (Gans 1980).

Methodology

This paper is based on semi-structured interviews conducted with journalists who have engaged with hacked data and materials from different reporting perspectives. The sample include reporters working across journalistic contexts, including general-interest news organizations, technology-focused publications, and investigative journalism outlets. Participants were selected for their experience in reporting on hacked information or their public engagement with the topic, such as speaking at journalism or cybersecurity conferences. In the context of this paper, sampled journalists have been chosen as representatives of a small but supranational area of contemporary journalism which is here analyzed as an example of “pioneer community” (Heep and Loosen, 2021), an emerging, innovative and still not entirely codified fraction of contemporary journalism.

Overall, 10 journalists have been included in the sample. Interviewees are based in various European countries and the United States. Within this framework, the geographic

concentration of the sample in Europe and North America reflects where this pioneer community has been most visibly constituted to date. These are the regions where this kind of journalism has been most visible, debated in journalism conferences and specialist publications, and most supported through investigative units and cyber-aware editorial cultures. This does not imply that these practices are absent elsewhere, as the aforementioned cases from Latin America suggest. Sampling from within this community is therefore consistent with the explorative logic of the study. It also reflects the interpretive demands of this kind of journalism, which is deeply embedded in local political cultures, legal disputes, and press freedom contexts that are difficult to read accurately from the outside. Future research should extend the geographic scope as the practice matures elsewhere.

Interviews were conducted in English via Zoom during the spring of 2025, with an average duration of approximately 40 minutes. All interviewees were granted full anonymity, including the withholding of nationality and affiliations, and their quotes are presented with pseudonyms. This reflects both explicit requests from participants, who cited concerns over retaliation, legal uncertainty, online harassment, and in some instances prior serious threats connected to their work, and the particular vulnerability of this cohort. Journalists working with hacked data form a small, highly specialized community, and even partial identifying information could plausibly lead to identification, especially in smaller countries or in politically sensitive cases where active practitioners are few and public visibility is high. The same level of protection was therefore applied uniformly across all participants, regardless of individual circumstances.

Interviews were recorded and later transcribed using the machine learning software Sonix.ai, before being edited by the author for clarity. Analysis was conducted through a deductive thematic analysis approach (Fereday and Muir-Cochrane 2006), selected for three reasons: the lack of prior literature on this specific area of inquiry within journalism studies, the exploratory nature of the study, and the aim of allowing journalists' own rationales and framings to emerge directly from the interview transcripts rather than being imposed by a pre-existing theoretical framework. Initial open coding was carried out using ATLAS.ti (Smit 2002), generating 46 codes. A subsequent process of manual clustering and merging was undertaken by the author to reduce redundancy and enhance conceptual coherence, grouping codes with overlapping content into 11 broader codes. These in turn were organized into five major thematic categories:

1) Digital landscapes and the emergence of hacked data journalism; 2) Hacker-journalist interactions and logics; 3) Reporting practices and verification strategies; 4) Negotiating trust and collaboration with hackers; and 5) Ethical considerations and professional boundaries.

In the results section that follows, each theme is illustrated through selected interview excerpts, chosen for their relevance and their capacity to capture the most significant insights from participants' perspectives.

Results

The five themes capture different dimensions of journalists' work with hacked data. Theme 1, "Digital landscapes and the emergence of hacked data journalism," reflects the broader political and technological context in which sampled journalists operate,

Table 1. Themes and codes emerging from the analysis.

Themes	Codes
1) Digital landscapes and the emergence of hacked data journalism	Emergence and growth; Intermediaries and political contexts
2) Hacker-journalist interactions and logics	Logics of access; Motivations and logics of hackers
3) Reporting practices and verification strategies	Selection and finding the story; Verification practices;
4) Negotiating trust and collaboration with hackers	Types of hacker sources; Source protection and trust; Comparisons with traditional sources
5) Ethical considerations and professional boundaries	Transparency and anonymity; Ethical decision-making

including the growth of reporting on hacked data and the role of digital intermediaries in facilitating it. Theme 2, “Hacker-journalist interactions and logics,” encompasses modes of access to hacked materials and the motivations of hacker sources. Theme 3, “Reporting practices and verification strategies,” covers how journalists select, frame, and verify hacked materials. Theme 4, “Negotiating trust and collaboration with hackers,” addresses source management and comparisons with more traditional journalistic sources. Theme 5, “Ethical considerations and professional boundaries,” captures questions of transparency and case-by-case ethical decision-making. Table 1 provides an overview of all codes included within each theme.

Digital Landscapes and the Emergence of Hacked Data Journalism

Emergence and Growth

Reporting on hacked data has emerged within a rapidly shifting technological and political landscape, and interviewees consistently described both the growing presence of hacked materials in their work and a diversification of the practices involved in handling them. Central to this expansion are a range of intermediaries, online spaces, hacker forums, Telegram channels, and dedicated leaking platforms such as Distributed Denial of Secrets (DDoS), which function simultaneously as technical infrastructures and historical reference points, alongside landmark moments such as the Snowden revelations and the WikiLeaks publications that continue to shape how journalists navigate this area of reporting.

These accounts underscore that reporting on hacked data is increasingly becoming routinized within the journalistic field, moving beyond technology reporting and gaining relevance across a wider range of journalistic domains, as most participants confirmed:

I would probably say it’s uncommon, but it has become more prevalent over the years. Before, it used to be a super niche thing, right? First, only a few journalists were paying attention to it, and second, data breaches were something only a relatively small group of journalists cared about. Now, you have these massive breaches, where you’re absolutely going to have journalists looking through that data, some of whom may have never dealt with hacked data before, but it’s because there’s such overwhelming public interest

(Erik)

Other journalists have noted how they regularly use hacked materials or online accessible repositories of hacked data as background information for their reporting, even when they aren’t working on a specific investigation related to the leaked data:

If you're looking into a person, like a criminal, a corrupt politician, or some shady individual, at least for me, I'll check. If I have an email address, I'll look it up in a database. It's become more mundane, just part of the process. Another reason why journalists are using it more is that a lot of these platforms now offer free access to journalists, which also helps a lot

(Kazu)

In one particularly striking instance, this convergence between hacking and journalism is not merely professional but biographical. One interviewee described a life trajectory that moved directly from hacking to journalism covering the same terrain:

I guess it probably has its roots in my own hacking when I was young. When I re-entered society after facing the consequences of that hacking, I eventually gravitated toward journalism. I was interested in a career that would allow me to investigate things that intrigued me, essentially the few lawful aspects of what I had been doing before, but without the criminal part

(Alex)

Interestingly, journalists have noted the existence of "two journalisms" related to reporting based on hacked materials. One reporter articulated this distinction in particularly clear terms:

On one hand, you have the traditional investigative journalists digging through large datasets from major leaks, who approach the material with the classic reporting toolkit, corroboration, interviews, contextualizing the data. (...) On the other hand, there's this newer, more technical niche where people work with constantly emerging, often smaller-scale data exposures, like scraping dark web dumps, pastebins, or unsecured cloud buckets, and turning those into fast-paced stories about breaches, vulnerabilities, and digital privacy. It's less about deep-dive investigation and more about monitoring and exposing ongoing data exposures in real time

(Robin)

On one side stands the established investigative tradition, where leaks are treated as raw evidence requiring contextualization and interpretation. On the other, a more monitoring-oriented approach prioritizes vigilance, technical literacy, and reporting on cyber incidents in their own right. The coexistence of these approaches illustrates how hacked data can be operationalized under different epistemic and professional logics. This framing suggests that the value of *hack-and-leak* instances lies not only in the exposure they can offer, but also in their capacity to be repurposed as evidence, transforming incidents into inquiries with broader societal implications. Yet this opportunity is also fraught, as the journalistic use of hacked materials raises crucial questions about legality, ethics, and responsibility in turning illicitly obtained data into legitimate news.

Intermediaries and Political Contexts

The interviews also highlight how the availability of hacked materials has expanded considerably over the past decade. What was once the domain of rare, large-scale leaks has now evolved into a flow of data exposures, sustained by the growing number of cyberattacks against companies, governments, and online platforms:

There's a lot more data out there on the internet today than there was ten years ago, like, a lot more. I think that's a big part of it: the amount of data, and the amount of information that companies and governments are putting online or making accessible, has increased significantly. As a result, hackers just have way more targets than they used to. I also think there's a lot going on in the world, and hacking is something you can do from wherever you are, with just a laptop

(Andrea)

This reflection points to a structural change: the vast expansion of digital infrastructures has multiplied both the attack surface for hackers and the volume of stolen data entering circulation, which in some cases has become a routinized source:

I think it's becoming increasingly common. For me, it's a bit hard to say exactly how common it is, because this is kind of my bread and butter, it's my beat to write about hackers, data breaches, and things like that. So, for me and my colleagues here at REDACTED, and even my former colleagues, it's almost a weekly occurrence

(Elliot)

Hacker–Journalist Interactions and Media Logics

Logics of Access

From the interviews, two distinct logics of accessing hacked materials emerge: a) *indirect*, through the growing availability of online data dumps and leaks, and b) *direct*, when hackers themselves approach journalists to share stolen information confidentially. The first mode involves journalists encountering data that hackers have independently released and publicized on the Internet, while the second reflects a more conventional source-reporter relationship in which hackers actively and directly provide materials to reporters. As will be discussed later in this paper, the second reporting scenario comes with considerably more repercussions and ethical concerns in terms of source protection, security and communication. Some journalists reported having equal experience of both approaches:

I've done plenty of both. The hack material that came to me directly was usually different in nature from what was publicly available, and it was always more interesting to me. I often felt a greater responsibility to cover it, whether I wanted to or not. On the other hand, if the information had already been leaked publicly and other reporters knew about it, I could pick and choose whether it was a story for me. Often, because of the nature of the material, I would spend time examining it for signs of where it came from or for any indications of inauthenticity

(Alex)

This account points to two distinct professional obligations that the mode of access activates: a heightened sense of editorial responsibility when materials arrive exclusively, and a more deliberate scrutiny of authenticity precisely because direct sources are harder to verify. Yet some journalists declined direct contact altogether, citing security concerns:

No, it's never happened that hackers just email us saying, 'Hey, you have this database.' I think we probably do get emails like that in general, but our rule is never to open them because

they might contain viruses, and we don't know who the sender is (...) If the data isn't available to everyone, then we don't use it.

(Kazu)

Motivations and Logics of Hackers

Journalists consistently noted a growing willingness among hackers to seek publicity and recognition for their actions and media exposure. Rather than simply posting stolen information online, many hackers now approach reporting strategically, aiming to be visible in news coverage and the broader public sphere:

I'd say that actors of all kinds love to flex and get credit. A lot of them don't, but many absolutely do. I'm not sure if the desire to flex has increased, but you've definitely seen the maturity of some hackers in how they approach the media. It's not just about posting things to Twitter like it might have been before

(Erik)

The "maturity" referenced here signals a strategic engagement with journalism in which hackers take into account how journalists will interpret, frame, and disseminate their materials, effectively leveraging media logic to enhance their visibility and influence:

I think hackers are starting to realize that they don't always need to go to someone like me—they can go to journalists working in other fields, depending on the story. In a way, it all goes back to Wikileaks. They partnered with journalism organizations and helped popularize the use of stolen materials for reporting

(Elliot)

Hackers choose their reporters deliberately, matching the leak to the journalist most likely to carry it furthest. That calculation is not equally sophisticated across all actors, however, and the sharpest divide runs between cybercriminal and state-affiliated groups:

If you look at the whole history of hacking, hackers have always had an element of attention-seeking. But you can often tell the difference between a genuine hacker leaking information they accessed and state-sponsored hackers. Real hackers are usually focused on the hack itself, how they did it, and when they release information to a reporter, it's mainly to demonstrate their access and the potency of the data they obtained. State-sponsored hackers are more direct about their intentions. They often highlight specific information because of their operation, and sometimes even offer to provide more data or targeted information. Because genuine, traditional hackers tend to have a strong ego component that's hard to replicate, it makes it somewhat easier to distinguish between the two

(Alex)

Reporting Practices and Verification Strategies

Selection and Finding the Story

In the interviews, journalists described a range of reporting practices, editorial decisions, and framing strategies used when covering hacked materials, highlighting the diversity and heterogeneity of the field. Most of these differences emerge as connected to the kinds of hackers involved and their alleged motivations. A key axis of variation concerns

whether the hack itself constitutes the news or merely enables it. When cybercriminals are involved, for instance, foregrounding their actions risks amplifying their leverage:

It's tricky because these actors are trying to monetize stolen data and pressure companies to pay. In those situations, it's usually better just to report that the company was hacked, without giving the hacker too much of a platform or attention unless necessary

(Elliot)

By contrast, when the breach exposes security weaknesses in prominent or socially significant actors, the hack-as-news logic operates differently, and the content of the breach may itself become secondary to the fact of it:

Sometimes, simply the fact that a company has been breached is newsworthy. Cyber criminals will give you data to show a company's been hacked. Ultimately, though, I might not even report on the hacked material itself, you know? Because, like, it's user data, email addresses, and passwords, or something like that. There's not much to dig through there journalistically. But there is enough to say, 'Oh, XYZ company was hacked,' and that's important because ABC

(Erik)

Hacked materials can also be employed as background rather than as the central focus of a story, providing context or corroboration without foregrounding the hack itself. As one interviewee noted plainly, the "smoking gun" does not always emerge directly, as "it's difficult to just find the wrongdoing in a database" (Kazu). For most of the journalists, the techniques used to report on hacked data are not very different from those applied in other reporting contexts and do not involve distinct computational methods. Information security practices are largely the same as those applied under other investigative circumstances, but with greater caution:

And especially in cases like ransomware, we usually rely on Tails and run it on computers without hard drives. We access the data through Tor and take other precautions to ensure our tracks remain hidden. This also helps contain any potential malware: if something infects the system, it only affects the USB stick, without access to anything else on the machine. That's an important safeguard, particularly when handling this type of high-risk data.

(Dominique)

Verification Strategies

All interviewed journalists stressed the central importance of verifying hacked data. Given the sensitive and controversial nature of hacked materials, they approach such sources with more skepticism. One journalist expressed this succinctly: "First of all, I treat them all as if they have chlamydia" (Nico). Yet verification practices per se are largely conventional, relying more on straightforward digital literacy than on advanced technical skills:

There are also some clever verification techniques I've learned. For example, if you have an email and password from the breach, it's unethical and often illegal to log in using those credentials. But you can try to sign up for the service with that email, often the site will say 'account already exists,' which indirectly confirms the email is in the company's database.

This doesn't expose any data but helps verify if the data is real. Some sites don't give that information, but, when possible, it's a useful technique

(Elliot)

Hacker-Journalist Relationships and Source Management

Types of Hacker Sources

The interviewed journalists emphasized the different types of hackers who may become sources. While the hacker world is historically not easy to categorize, cybercriminals, hacktivists, and state-affiliated actors all can play a role in this landscape, and the distinctions between them carry significant implications for how journalists build relationships with them. Rather than a neat taxonomy, what emerges from the interviews is a picture of overlapping motivational profiles that can coexist and blur within the same actor:

There's like these different types of hackers that exist that I think it's an interesting phenomenon where you have these people that are driven by technological curiosity, and they like to hack things for the sake of hacking things. And they're super nerdy and they just see something that is not 100% secure, so they have to get into it. And then in the end, they almost use the journalism as an excuse for for the hacking hobby, because when they find something, they justify what they did. Then there's this other group that is motivated by financial gain. And then you have these state actors in there as well

(Moor)

A distinctive area of reporting concerns surveillance companies that develop abusive software. In some instances, these firms have been hacked and exposed by hacktivist groups seeking to reveal their opaque business practices:

In fact, spyware companies have been hacked multiple times in the last ten years. Over the last five years, I think there have been around 26 such companies hacked. These breaches are particularly sensitive because these companies are clearly problematic. Most of them market their products, some explicitly, others less so, to jealous partners looking to spy on boyfriends, girlfriends, or spouses without their consent. These companies collect a lot of sensitive data without the victim's knowledge or consent, and when they get hacked, the privacy of these people is exposed. That's why you must be very careful in covering these stories. But there is public interest in exposing these companies, not only because they enable spying without consent, which is essentially criminal, but also because they fail to protect the data they collect, allowing others to steal information that's already been illicitly gathered

(Elliot)

Journalists expressed a range of perspectives on the types of hackers they encountered. For some, their interactions were primarily with cybercriminals:

I would say most of them, for me, are going to be cyber criminals. After that, it's probably going to be hacktivists or activists. I think relatively rarely it's going to be state actors, like part of some kind of misinformation, disinformation, or influence campaign. Right? And those aren't that frequent, at least in the breaches I cover. But yeah, mostly cyber criminals

(Erik)

For others, it is still a field dominated by political hackers, either hacktivist or state-affiliated:

Yeah, I think it's more often the state-sponsored hackers and hacktivists with political goals who reach out to journalists. Cybercriminals usually aren't motivated to bring public attention to issues. Instead, they put things on forums or the dark web to sell or blackmail, finding their customers that way. So, it's mainly hacktivists and state-sponsored actors with political agendas who contact journalists

(Kai)

Source Protection and Trust

Source protection emerged as the most debated issue among the interviewed journalists. Some extend full source protection to hackers, just as they would to any other source, including whistleblowers:

I won't publish anything in the article that could lead to their identification, and I won't provide information to their staff as a whistleblower. And for a cybercriminal, I'm not going to give information to the police that would help them investigate or apprehend them. This is a source, and I'm going to protect them (...) I've been asked plenty of times by law enforcement to provide information about hackers or criminals I've spoken to, and obviously, I've always refused

(Erik)

Other journalists, while still attentive to source protection, prefer to know as little as possible about the hackers they rely on, framing this as a harm-reduction strategy that minimizes risk for both parties:

The less I know about these things, the harder it's going to be for me to burn my source or to publish something that inadvertently turns out to be harmful to my source

(Moor)

Others, particularly those who work only with hacked materials already openly available online, tend to be less concerned with source protection, as the origins of the materials are often impossible to trace:

We would consider it that much for their safety because these platforms usually, especially telegram ones like you have no idea who is behind them (...) For me personally, like, I wouldn't think much about their protection

(Kazu)

Comparisons with Traditional Sources

The discussion of source protection also generated comparisons between hacker sources and whistleblowers, producing a wide spectrum of views. Some emphasized the fundamental difference in status, while still acknowledging parallels in how they are handled. Legal repercussions were also a recurring theme, along with the question of source motivation:

It's not the same, because legally it's completely different. Working with material that I know, or strongly suspect, to be hacked carries very different legal implications than working with a whistleblower. In a whistleblower situation, ideally the individual has legal advice or is connected to a whistleblower organization, with some structure and context around the process of handing over the material. That support makes it easier for me to work both with the

person and with the documents. And let's be honest, there's also the question of motivation. What drives someone to take this step? To go down this road? That, in itself, is an interesting part of the journalistic story

(Moor)

Others argued that the suspicion directed at hacker sources reflects a double standard, given that more routinized source relationships carry their own unexamined problems:

I think those suspicious of working with hacker sources may not be fully honest about the flaws of the other sources they work with. Hackers have complicated motivations, and it's often harder to evaluate them because you're usually talking to anonymous people who you only know through what they tell you. I understand why journalists prefer meeting sources in person, not on encrypted chat apps, but that's the reality now

(Kai)

Ethical Considerations and Professional Boundaries

Transparency and Anonymity

Source protection was not the only ethical issue raised by journalists. The sample also discussed broader questions related to the ethics of reporting, including their own transparency and the anonymity of their sources. Several journalists reflected on how much of their investigative process they should reveal to audiences, and debated the extent to which information about sources, even when anonymized, should be disclosed when handling highly sensitive or hacked materials. Some claim they should always be as transparent as possible while protecting sources:

I think it's best to be as transparent as you can while protecting your source. Ideally, you would be completely transparent, you would explain everything, like how you were contacted, how you got the data, and who the source is, ideally. But in many cases, you can't say that. This is one of the reasons why it's safer to report on hacked data than on whistleblowers: you can say something like, 'A hacker did this; I don't know who they are.' That's a much better position to be in

(Andrea)

The preferences and intentions of hacker sources were also identified as a decisive factor in calibrating transparency:

I think you can be quite transparent, and there's really no reason not to be. For example, if a hacker approaches you and asks to keep their identity private, whether they're cybercriminals or not, you must respect that. But beyond that, it's often better to err on the side of transparency. (...) Sometimes cybercriminals post their hacks on forums where they advertise stolen data and set a price. In those cases, it's part of the story to say that the hacker is trying to sell the data. Being open about this helps journalists distance themselves from the hacker's motives

(Elliot)

These transparency demands become still more acute when source identity cannot be established with confidence, a challenge that is most acute when state-affiliated actors may be masquerading as independent hacktivists to lend credibility to politically motivated leaks:

I think you should be very transparent about that in your reporting. You should say something like, 'we don't know who the source is; it could be the GRU or whoever, but we have confirmed that this data is real and this is what it shows'

(Andrea)

This is not a merely theoretical concern, cases of state actors posing as independent hacktivists are well documented:

I also think it happens pretty frequently that state-sponsored groups pretend to be hacktivists. The big case study for that is Guccifer 2.0, WikiLeaks, and everything surrounding that, they were pretending to be hacktivists too

(Andrea)

Ethical Decision-Making

Journalists discussed the decision-making involved in determining whether to publish a story based on hacked data. In particular, they reflected on how to balance the public interest in the materials with the fact that sources may have operated illegally or may not be motivated by the public good. Newsworthiness and public interest were frequently cited as the most decisive factors:

I'm sure different people have different views, but I kind of think it all depends on what you're exposing. Maybe it's generally wrong to break into people's computers and steal data, but if you're exposing serious crimes, then I think it can be justified

(Andrea)

Journalists working in this space converge on an unusual position: that the decision cannot be proceduralized, and that judgement in the individual case is the only workable standard:

At the same time, it's problematic to say the public interest only exists if something happens to coincide with your own worldview. So, I think it's hard to answer these questions in the abstract. You really must look at each case individually, what it's saying and what the specific questions are

(Robin)

Taken together, the five themes reveal a field in which established journalistic norms, verification, source protection, transparency, and public interest are being actively renegotiated rather than abandoned, as journalists adapt familiar professional frameworks to the distinctive legal, ethical, and epistemic pressures that hacked data introduces.

Conclusion and Discussion

The results show a multifaceted scenario that, given its controversies and inherent risks, positions journalists within complex reporting situations requiring *case-by-case* decisions. Hacked data reporting is evolving from a *fringe* practice into a more established and normalized aspect of contemporary reporting, driven by high-profile leaks, intermediaries such as platforms and forums, and the growing free availability of digital data online. Journalists report accessing materials either indirectly, through publicly released repositories,

or directly when hackers approach them, with the latter raising greater ethical, legal, and security concerns. Their practices generally follow conventional journalistic methods, emphasizing verification and information security, while sometimes requiring specialized technical precautions unique to cyber-related materials. The hackers who become sources vary widely, from cybercriminals to hacktivists and state-affiliated actors, demanding nuanced approaches to engagement, trust, and source protection: some journalists extend whistleblower-style protection, while others minimize knowledge of sources or rely solely on public materials to reduce risk. Ethical considerations—transparency, source anonymity, and the balancing of public interest against illegal or self-serving motives—are likewise managed largely on a case-by-case basis.

These findings advance the literature in three ways. First, no previous study has offered a sustained empirical account of how journalists negotiate sourcing relationships with hackers and of the rationales underpinning that work. This paper provides a first such account, documenting how journalists acknowledge and draw on the contributions hackers can bring while managing the attendant risks. Second, it maps a small but emerging and highly significant niche of reporting that blends investigative journalism, information security, and technology reporting into a distinctive practice not reducible to any of them. Third, by showing how journalists handle materials whose origins are illicit, whose sources are often anonymous, and whose motives are frequently opaque, it further complicates the ethical tensions that characterize contemporary digital journalism, while highlighting the complexities of these environments and the challenges they pose to the profession more broadly.

Reporting based on hacked data thus confirms the complexity and fluidity of journalism under datafication, requiring journalists to navigate legal, moral, and practical challenges while transforming illicitly obtained data into public knowledge. The results exemplify a further hybridization between traditional journalistic practices and hacker logics, in which the circulation of stolen data, engagement with the press, and digital acts of disclosure shape news production, at times in dysfunctional and controversial ways. This model points to a notable reflexivity: journalists adapt to the fast-changing and ethically ambiguous world of cyberspace, while hacker practices, intermediaries, and digital infrastructures increasingly structure reporting routines, shape editorial decisions, and amplify public attention, in addition to providing access to source materials. Seen this way, hacked data reporting suggests not only an evolution of investigative practice but also a mirror of the contemporary Internet, revealing its patterns, vulnerabilities, and power dynamics.

Several limitations should be acknowledged. The sample of ten interviewees constrains generalization and supports analytic rather than statistical claims, and the snowball recruitment through publicly visible practitioners necessarily selects for a particular kind of “pioneer,” under-representing those who avoid public-facing engagement. The concentration of participants in Europe and North America further limits transferability, as does the conduct of interviews in English, which excludes practitioners working primarily in other linguistic spheres. The findings also rest on self-report rather than newsroom observation, capturing how journalists narrate their practice rather than that practice as directly observed, and the dataset does not include the editors, in-house lawyers, or hacker sources who likewise shape the decisions discussed. Finally, the study offers a snapshot of a fast-moving field as of spring 2025; given how rapidly this panorama is

changing, some of its dynamics may already have shifted, and its thematic frame may have under-captured developments that a more inductive analysis would surface.

Different trajectories for future research also follow. Extending the analysis to a wider range of national contexts, particularly beyond Europe and North America, would test how far these practices travel under different legal regimes and press-freedom conditions, building on emerging cases from the Global South. Broadening the scope across additional reporting beats would clarify whether these dynamics hold as hacked data becomes embedded in fields beyond technology and cybersecurity reporting. Future work might also examine how AI-related digital threats, from synthetic media to AI-assisted intrusions, reshape the verification practices documented here, while more focused studies of cybercrime or state-sponsored hacking as journalistic sources would allow closer attention to the distinct challenges each poses. Finally, further normative and empirical work should address the ethics of this practice, taking up the case-by-case judgment documented here and asking what professional guidance could support such discernment without reducing it to rigid codes ill-suited to the dilemmas hacked data presents.

This form of reporting therefore functions both as a product of and a lens onto the contemporary digital landscape, suggesting how journalism and a turbulent cyberspace increasingly co-constitute each other. As the boundaries between actors and information flows continue to blur, covering hacked data is likely to become further embedded in wider reporting on datafication and cyber conflict, calling for renewed scholarly and professional attention to the ethical frameworks, institutional safeguards, and interpretive skills such contested materials demand. Ultimately, hacked data reporting points to a broader reconfiguration of epistemic authority in the digital age, in which journalists act as mediators within a complex ecosystem of leaks and opaque digital actors, shaping public understanding under conditions of uncertainty, volatility, and asymmetric power.

Acknowledgments

An earlier version of this paper was presented at the 2025 Future of Journalism Conference in Cardiff. My thanks to the panel participants and to the conference community for their questions and comments, which improved the argument considerably.

Author Contributions

CRedit: **Philip Di Salvo:** Conceptualization, Formal analysis, Investigation, Methodology, Writing – original draft, Writing – review & editing.

Disclosure Statement

The author reports there are no competing interests to declare.

AI Disclosure Statement:

The author used Claude Opus 4.7 to revise the manuscript's language for clarity and to assist in identifying literature for parts of the literature review. All intellectual decisions, data, and substantive content remain those of the author.

Funding

The author received no specific funding for this research

References

- Altheide, D. L. 2015. "Media Logic." In *The International Encyclopedia of Political Communication*, edited by G. Mazzoleni, 1–6. Hoboken, NJ: Wiley-Blackwell.
- Araujo, R., and C. Belim. 2024. "Journalistic Coverage of a Political Scandal in Democracy: Vaza Jato in Folha de S.Paulo." *Brazilian Journalism Research* 20 (3): e1673. <https://doi.org/10.25200/BJR.v20n3.2024.1673>.
- Barr, J., and S. Liemann Escobar. 2023. *Hacktivism in Latin America: The Case of Guacamaya. Digital Security in Latin America Research Group, Royal Holloway*. London: University of London.
- Berkowitz, D. 2019. "Reporters and Their Sources." In *The Handbook of Journalism Studies*, edited by K. Wahl-Jorgensen and T. Hanitzsch, 165–179. London: Routledge.
- Carlson, M. 2009. "Dueling, Dancing, or Dominating? Journalists and Their Sources." *Sociology Compass* 3 (4): 526–542. <https://doi.org/10.1111/j.1751-9020.2009.00219.x>
- Carlson, M. 2016. "Metajournalistic Discourse and the Meanings of Journalism: Definitional Control, Boundary Work, and Legitimation." *Communication Theory* 26 (4): 349–368. <https://doi.org/10.1111/comt.12088>
- Carlson, M., and S. C. Lewis. 2015. *Boundaries of Journalism: Professionalism, Practices and Participation*. London: Routledge.
- Coleman, G. 2015. *Hacker, Hoaxer, Whistleblower, spy: The Many Faces of Anonymous*. London: Verso books.
- Coleman, G. 2017a. "The Public Interest Hack." *Limn* 1:8.
- Coleman, G. 2017b. "From Internet Farming to Weapons of the Geek." *Current Anthropology* 58 (S15): S91–S102. <https://doi.org/10.1086/688697>
- Crete-Nishihata, M., J. Oliver, C. Parsons, D. Walker, L. Tsui, and R. Deibert. 2020. "The Information Security Cultures of Journalism." *Digital Journalism* 8 (8): 1068–1091. <https://doi.org/10.1080/21670811.2020.1777882>
- Di Salvo, P. 2020. *Digital Whistleblowing Platforms in Journalism: Encrypting Leaks*. London: Palgrave Macmillan.
- Di Salvo, P. 2024. "A Typology of Digital Leaks as Journalistic Source Materials." In *The Palgrave Handbook of Everyday Digital Life*, edited by H. S. Dunn, M. Ragnedda, M. L. Ruiiu, and L. Robinson, 469–488. Cham: Springer International Publishing.
- Duffy, M. J., and C. P. Freeman. 2011. "Anonymous Sources: A Utilitarian Exploration of Their Justification and Guidelines for Limited Use." *Journal of Mass Media Ethics* 26 (4): 297–315. <https://doi.org/10.1080/08900523.2011.606006>
- Dutton, W. H. 2023. *The Fifth Estate: The Power Shift of the Digital age*. Oxford: Oxford University Press.
- Elliott, C. 2013. "WikiLeaks and the Public Interest Dilemma: A View from Inside the Media." In *Beyond WikiLeaks: Implications for the Future of Communications, Journalism and Society*, edited by B. Brevini, A. Hintz, and P. McCurdy, 78–84. London: Palgrave Macmillan.
- Ericson, R. V., P. M. Baranek, and J. B. Chan. 1989. *Negotiating Control: A Study of News Sources*. Toronto: University of Toronto Press.
- Fereday, J., and E. Muir-Cochrane. 2006. "Demonstrating Rigor Using Thematic Analysis: A Hybrid Approach of Inductive and Deductive Coding and Theme Development." *International Journal of Qualitative Methods* 5 (1): 80–92. <https://doi.org/10.1177/160940690600500107>
- Fisher, C. 2023. "News Sources and Journalist–Source Interaction." *Oxford Research Encyclopedia of Communication*. <https://academic.oup.com/edited-volume/61798/chapter-abstract/546233643?redirectedFrom=fulltext>.
- Gans, H. J. 1980. *Deciding What's News: A Study of CBS Evening News, NBC Nightly News, Newsweek, and Time*. New York: Vintage Books.
- Gates, K. 2020. "Media Evidence and Forensic Journalism." *Surveillance & Society* 18 (3): 403–408. <https://doi.org/10.24908/ss.v18i3.14090>

- Heinrich, A., and P. L. Spyridou. 2025. "Digital Sourcing." In *The Routledge Companion to Digital Journalism Studies 2nd ed*, edited by S. A. Eldridge II, D. Cheruiyot, S. Banjac, and J. Swart, 299–308. London: Routledge.
- Hepp, A., and W. Loosen. 2021. "Pioneer Journalism: Conceptualizing the Role of Pioneer Journalists and Pioneer Communities in the Organizational re-figuration of Journalism." *Journalism* 22 (3): 577–595. <https://doi.org/10.1177/1464884919829277>
- Hepp, A., and W. Loosen. 2021. "Pioneer Journalism: Conceptualizing the Role of Pioneer Journalists and Pioneer Communities in the Organizational Re-Figuration of Journalism." *Journalism* 22 (3): 577–595. <https://doi.org/10.1177/1464884919829277>.
- Hosaka, S. 2025. "Leaked Email Data: A new Source for the Study of Authoritarian Regimes." *Digital War* 6 (1): 1. <https://doi.org/10.1057/s42984-024-00097-w>
- Jordan, T. 2017. "A Genealogy of Hacking." *Convergence: The International Journal of Research into New Media Technologies* 23 (5): 528–544. <https://doi.org/10.1177/1354856516640710>
- Khan, S. A., L. Dierickx, J. G. Furuly, H. B. Vold, R. Tahseen, C. G. Linden, and D. T. Dang-Nguyen. 2025. "Debunking war Information Disorder: A Case Study in Assessing the use of Multimedia Verification Tools." *Journal of the Association for Information Science and Technology* 76 (5): 752–769. <https://doi.org/10.1002/asi.24970>
- Kovach, B., and T. Rosenstiel. 2021. *The Elements of Journalism: What Newspeople Should Know and the Public Should Expect*. 4th ed. New York: Crown.
- Lee, M. 2024. *Hacks, Leaks, and Revelations: The art of Analyzing Hacked and Leaked Data*. San Francisco: No Starch Press.
- Lewis, S. C., and N. Usher. 2016. "Trading Zones, Boundary Objects, and the Pursuit of News Innovation: A Case Study of Journalists and Programmers." *Convergence: The International Journal of Research into New Media Technologies* 22 (5): 543–560. <https://doi.org/10.1177/1354856515623865>
- Lin, H. 2022. "Russian Cyber Operations in the Invasion of Ukraine." *The Cyber Defense Review* 7 (4): 31–46.
- Marmura, S. M. 2018. *The WikiLeaks Paradigm: Paradoxes and Revelations*, 109–133. Cham: Springer International Publishing.
- Maynard, P., and K. McLaughlin. 2020. "Big Fish, Little Fish, Critical Infrastructure: An Analysis of Phineas Fisher and the 'Hacktivist' threat to Critical Infrastructure." In *2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)*, 1–7. London: Centre for Multidisciplinary Research, Innovation and Collaboration (C-MRIC).
- McGregor, S. E. 2021. *Information Security Essentials: A Guide for Reporters, Editors, and Newsroom Leaders*. New York: Columbia University Press.
- Meissner, F., A. J. Wilke, and M. Puikytė. 2025. "How Is Cybersecurity Discussed across Media Channels? Exploratory Analyses of Twitter Content and News Reporting." *Journal of Risk Research* 28 (8): 855–875. <https://doi.org/10.1080/13669877.2025.2553079>
- Philp, R. 2023, November 28. "Working with Hackers: Where — and How — Journalists Should Use These Sources." *Global Investigative Journalism Network*. <https://gijn.org/stories/best-practices-investigating-hacked-data/>.
- Plaisance, P. L. 2018. "Journalism Ethics." In *Journalism*, edited by T. P. Vos, 83–105. Berlin: Walter de Gruyter Inc.
- Porlezza, C. 2018. "Deconstructing Data-Driven Journalism." *Reflexivity between the Datafied Society and the Datafication of News Work. Problemi Dell'informazione* 43 (3): 369–392.
- Porlezza, C. 2024. "The Datafication of Digital Journalism: A History of Everlasting Challenges between Ethical Issues and Regulation." *Journalism* 25 (5): 1167–1185. <https://doi.org/10.1177/14648849231190232>
- Ross, A. 1990. "Hacking Away at the Counterculture." *Postmodern Culture* 1:1. <https://doi.org/10.1353/pmc.1990.0011>
- Ruohonen, J., K. Hjerpe, and M. Von Zastrow. 2024. "An Exploratory Case Study on Data Breach Journalism." In *Proceedings of the 19th International Conference on Availability, Reliability and Security*, 1–9. New York: Association for Computing Machinery. <https://dl.acm.org/doi/proceedings/10.1145/3664476>.

- Sanders, K. 2003. *Ethics and Journalism*. London: SAGE Publications.
- Sauter, M. 2017. "The Illicit Aura of Information." *Limn* 1 (8): 51–56. <https://limn.it/articles/the-illicit-aura-of-information/>.
- Schaetz, N., J. A. Lischka, and L. Laugwitz. 2025. "Datafication of Journalism: How Data Elites and Epistemic Infrastructures Change News Organizations." *Digital Journalism* 13 (4): 677–695. <https://doi.org/10.1080/21670811.2023.2235601>
- Scott, B. 2024. "Everyone Freaks out When the Leaks Are Made": Data Leaks, Investigative Journalism and Intelligence Practice." *Journal of Financial Crime* 31 (3): 545–557. <https://doi.org/10.1108/JFC-05-2023-0123>.
- Shapiro, S. 2023. *Fancy Bear Goes Phishing: The Dark History of the Information age, in Five Extraordinary Hacks*. New York: Random House.
- Sigal, L. V. 1973. Reporters and Officials: The Organization and Politics of Newsmaking. D. C. Heath.
- Smit, B. 2002. "Atlas.ti for Qualitative Data Analysis." *Perspectives in Education* 20 (3): 65–75.
- Steel, J., J. Firmstone, M. Conboy, C. Fox, C. Elliott-Harvey, J. Mulderrig, J. Saunders, and P. Wragg. 2025. "Journalism and Ethical Praxis: A Thematic Analysis of Journalism Ethics across Five European Countries." *Journalism Practice*, <https://doi.org/10.1080/17512786.2025.2480746>.
- Thomas, R. J. 2018. "Harm in Journalism." In *Communication and Media Ethics*, edited by P. L. Plaisance, 215–234. Berlin: De Gruyter Mouton.
- Träsel, M. 2018. "Hacks and Hackers: The Ethos and Beliefs of a Group of Data-Driven Journalism Professionals in Brazil." *Revista FAMECOS* 25 (1): 1–14.
- Usher, N. 2018. "Hacks, Hackers, and the Expansive Boundaries of Journalism." In *The Routledge Handbook of Developments in Digital Journalism Studies*, edited by S. Eldridge II and B. Franklin, 348–359. London: Routledge.
- Vanacker, B. 2021. "Ethical Issues in Data Journalism." In *The Routledge Companion to Journalism Ethics*, edited by L. T. Price, K. Sanders, and W. N. Wyatt, 301–309. London: Routledge.
- Van Der Woude, M., T. Dodds, and G. Torres. 2025. "The Ethics of Open Source Investigations: Navigating Privacy Challenges in a Gray Zone Information Landscape." *Journalism* 26 (10): 2184–2202. <https://doi.org/10.1177/14648849241274104>
- Ward, S. J. 2015. *Radical Media Ethics: A Global Approach*. Hoboken: John Wiley & Sons.
- Waters, S. 2020. "The Ethical Algorithm: Journalist/Whistleblower Relationships Explored through the Lens of Social Exchange." *Journalism & Communication Monographs* 22 (3): 172–245. <https://doi.org/10.1177/1522637920947719>.
- Westlund, O., R. Krøvel, and K. S. Orgeret. 2024. *Journalism and Safety: An Introduction to the Field*. Abingdon: Taylor & Francis.
- Wheatley, D. 2020. "A Typology of News Sourcing: Routine and non-routine Channels of Production." *Journalism Practice* 14 (3): 277–298. <https://doi.org/10.1080/17512786.2019.1617042>
- Whyte, C. 2020. "Cyber Conflict or Democracy 'Hacked'? How Cyber Operations Enhance Information Warfare." *Journal of Cybersecurity* 6:1. <https://doi.org/10.1093/cybsec/tyaa013>
- Zittrain, J. 2016. "Mass Hacks of Private Email Aren't Whistleblowing, They Are at Odds with It." *Just Security*. <https://www.justsecurity.org/33677/mass-hacks-private-email-arent-whistleblowing-odds-it/>.