Media and Communication (ISSN: 2183–2439)
2021, Volume 9, Issue 2, Pages 130–139
DOI: 10.17645/mac.v9i2.3804

Article

Mobile Journalists as Traceable Data Objects: Surveillance Capitalism and Responsible Innovation in Mobile Journalism

Anja Salzmann *, Frode Guribye and Astrid Gynnild

Department of Information Science and Media Studies, University of Bergen, N-5020 Bergen, Norway;
E-Mails: anja.salzmann@uib.no (A.S.), frode.guribye@uib.no (F.G.), astrid.gynnild@uib.no (A.G.)

* Corresponding author

Submitted: 30 October 2020 | Accepted: 25 January 2021 | Published: 6 April 2021

Abstract
This article discusses how Shosana Zuboff's critical theory of surveillance capitalism may help to understand and underpin responsible practice and innovation in mobile journalism. Zuboff conceptualizes surveillance capitalism as a new economic logic made possible by ICT and its architecture for extracting and trading data products of user behavior and preferences. Surveillance is, through these new technologies, built into the fabric of our economic system and, according to Zuboff, appears as deeply anti-democratic and a threat to human sovereignty, dignity, and autonomy. In Europe, the framework of responsible research and innovation is promoted as an approach and a meta-concept that should inform practice and policy for research and innovation to align with societal values and democratic principles. Within this approach, ICT is framed as a risk technology. As innovation in mobile journalism is inextricably tied to the technologies and infrastructure of smartphones and social media platforms, the apparent question would be how we can envision responsible innovation in this area. Zuboff provides a critical perspective to study how this architecture of surveillance impedes the practice of mobile journalism. While the wide adoption of smartphones as a key tool for both producing and consuming news has great potential for innovation, it can also feed behavioral data into the supply chain of surveillance capitalism. We discuss how potentially harmful implications can be met on an individual and organizational level to contribute to a more responsible adoption of mobile technologies in journalism.

Keywords
innovation; journalism; mobile journalism; mobile technology; responsible innovation; responsible research; risk technology; surveillance capitalism; Zuboff

Issue
This article is part of the issue "Critical Theory in a Digital Media Age: Ways Forward" edited by Robert E. Gutsche, Jr. (Lancaster University, UK).

1. Introduction

> Mojo is agile, it is affordable, it keeps a low profile, it is inspiring journalists around the globe to think outside the box. As such, it is the right tool to defend journalism in a world that finds itself in a prolonged state of emergency and will need to invent itself newly.

With these words, the German Konrad Adenauer Foundation (2020) introduced what they labeled the world's first virtual conference on mobile journalism. The aim of this foundation is to "promote and preserve free democracy and a social market economy" by engaging in the training of journalists toward "a free, ethical and responsible press" (Konrad Adenauer Foundation, 2020). The smartphone is promoted as an all-in-one device allowing journalists to create and edit photos, videos, audio, and graphics, which can then be directly uploaded to newsroom servers or disseminated to social media platforms.

Mobile journalism is a fast-growing field (Burum & Quinn, 2016; Duffy, 2011; Goggin, 2010; Perreault & Stanfield, 2018; Salzmann, Guribye, & Gynnild, 2020; Westlund & Quinn, 2018), and smartphone-based reporting is an emerging playground for media innovations (Palacios, Barbosa, da Silva, & da Cunha, 2016) that proposedly holds the potential to further democratize journalism (Burum, 2016; Duffy, 2011).

While low-cost, widespread mobile technologies have empowered journalists in their daily work (Belair-Gagnon, Agur, & Frisch, 2016; Molyneux, 2018; Westlund & Quinn, 2018), the same technologies can enable surveillance, control, and censorship (Pavlik, 2019). Smartphones are equipped with capabilities to collect comprehensive data traces from users that can be aggregated and triangulated into complex individual profiles (Christl, Kopp, & Riechert, 2017a; Christl & Spiekermann, 2016). From the perspective of Zuboff's surveillance capitalism, mobile technologies can be perceived as a centerpiece of a surveillance architecture that has been developed as part of a new arising economic logic (Zuboff, 2019). One of the key challenges in understanding the implications of surveillance capitalism for mobile journalism is that surveillance practices do not target journalists specifically, but are equally applied to all citizens that rely on new digital platforms and tools. Therefore, many of the consequences and the potential harm will not be exclusive to journalists. Journalists, however, are a risk group, and the risks are potentially higher for this group.

Zuboff's theory can serve as a lens through which one can understand the societal implications of an emerging economic logic based on advanced algorithms and the extensive exploitation of behavioral data. Nonetheless, it does not address, in a systematic manner, how these challenges can be resolved. Thus, the question arises: How can mobile journalism and innovation in this field be practiced responsibly in the context of convergent technologies and pervasive surveillance structures? In this article, we discuss whether the European policy strategy Responsible Research and Innovation (RRI) might be a suitable approach to address key issues related to the responsible adoption of mobile technology in journalism and to guide innovation in the field of mobile journalism.

The aim of this article is twofold. First, we reflect critically on how the theory of surveillance capitalism impedes the field of mobile journalism and how this architecture of surveillance might threaten media freedom, which might ultimately undermine fundamental democratic values. Second, we outline the European RRI approach as a framework for societal action and a way to evoke social engagement on challenges arising through the adoption and development of risk technologies. We first introduce Zuboff's theory on surveillance capitalism, followed by a discussion on mobile journalism from the perspective of Zuboff's theory, where we identify challenges of surveillance capitalism for journalistic practice and innovation. Next, we introduce the RRI approach, followed by outlining major implications for mobile journalism on an individual and organizational level and how they might be responsibly approached.

2. Zuboff's Theory of Surveillance Capitalism

In her seminal book *In the Age of the Smart Machine: The Future of Work and Power*, Shoshana Zuboff (1988) investigated computer-mediated work in organizational work processes and identified what she outlined as the fundamental duality of information technology. Information technology, according to Zuboff, not only has the capacity to automate but also 'informate' by producing and generating new information and giving insights about processes and activities that were previously invisible or unavailable.

In Zuboff's (2019) recent book, she traced the development, strategies, and research ambitions of American technology companies like Google, Facebook, and Microsoft, which in her view served as 'petri dishes' to examine 'the DNA' of this new arising economic logic that she terms 'surveillance capitalism' (p. 24). Zuboff's (2019) theory is based on an extensive collection of empirical material and combines qualitative social science methods with historical and philosophical approaches.

To grasp the new surveillance paradigm, she developed a conceptual framework to describe this new economic logic and its broader societal consequences. In particular, Zuboff (2016, 2019) considers Google a pioneer of surveillance capitalism. Google discovered very early that they could capitalize on so-called data byproducts. These data byproducts generated traces and logs of users' interactions with Google's products, and services could be aggregated and analyzed not only to help the company provide better services, but also to, for example, offer tools for data analytics, as well as deliver targeted ads and what Zuboff terms 'behavioral products.' Thus, this raw data was seen as an important asset of great economic value. Zuboff calls these data byproducts 'behavioral surplus' (Zuboff, 2019, p. 8). These new data products can be applied for a multitude of purposes. In Zuboff´s terminology, they are 'surveillance assets' (p. 81), based on the idea of human experience as free raw material that can be translated into behavioral data (p. 179) and used "to predict and modify human behavior to produce revenue and market control" (Zuboff, 2015, p. 75). The discovery of these new prediction products triggered the rise and institutionalization of a new economic logic that translates into a new widespread business model, leading to a more radical "parasitic and self-referential form" of capitalism (Zuboff, 2019, p. 9) that centers on this large-scale data collection and the commodification of personal data (Zuboff, 2016, 2019).

While the commodification of personal data and the prediction of human behavior were at first a means for targeted advertising, they later became a means for what Zuboff (2019) sees as the next level of a new 'prediction imperative' (Zuboff, 2019, p. 197) and referred

to as 'economies of action' (Zuboff, 2019, p. 293–299). The real-time data of human behavior could be analyzed instantly and used for "ubiquitous intervention, action, and control" (p. 293), subsequently leading to what she calls new means of 'behavior modification' (Zuboff, 2019, p. 293). Zuboff claims that people are unaware of the commodification of their data, and processes and established infrastructures are mostly invisible, difficult to trace, willingly obscured by surveillance capitalists themselves, and thriving on the public's ignorance.

According to Zuboff, another characteristic that marks surveillance capitalism is what she calls 'radical indifference' (Zuboff, 2019, p. 376–377), where "content is judged by its volume, range, and depth of surplus as measured by the 'anonymous' equivalence of clicks, likes, and dwell times, despite the obvious fact that its profoundly dissimilar meanings originate in distinct human situations" (p. 505). In other words, the algorithmic logic of surveillance capitalism is indifferent about what users of services and products say, think, or do. What matters the most is that human interactions can be converted into data (Zuboff, 2015, p. 211–212), and the ultimate goal of the actors is to maximize traffic on their platforms so they can collect as much data as possible. The data representations of user behavior are, in a certain sense, indifferent whether they accurately mirror the objects represented. The representations and algorithmic analysis of the data, rather, take on a value and a life of their own, depending more on utility in this new economic logic (see also Nassehi, 2019).

Zuboff (2019) also points out how big corporations such as Google and Facebook have inserted themselves as intermediaries between media publishers and their audiences. Their algorithmically steered processes are, according to Zuboff, marked by a radical indifference of equivalence-steered and self-referential data algorithms, which she also calls "a new way of knowing" (p. 376) and describes as a form of "observation without witnesses" (p. 377). According to Zuboff (2019), this new logic can be observed in social media feeds and efforts of content standardization, ranking fake news stoically as proven scientifically or journalistically produced facts and figures. Journalism, in contrast, represents for Zuboff "the precise opposite of this logic" (p. 507), claiming that journalism is based on 'organic reciprocity' (p. 507) in its interactions with audiences. In other words, journalism is not a one-sided affair like the extraction of data that commodifies people's behavior.

For Zuboff, the institutionalization of this new economic logic represents a fundamental change in basic assumptions from the 20th century industrial society, organized around the division of labor and work as a central force of production to a division of learning in the digital age of the 21st century (Zuboff, 2015, 2019). Surveillance capitalism, Zuboff argues, establishes a new and unprecedented 'instrumentarian power' (Zuboff, 2019, pp. 67, 376–379), reflected by emerging asymmetries and the concentration of knowledge and rights. Companies like Google, Facebook, Amazon, and Microsoft have become what Zuboff calls "surveillance empires that exercise total control over the world's information" (Zuboff, 2020), as they own the algorithms, research, and knowledge that form the backbone of their digital infrastructures and services.

Most prominently, Zuboff's theory has been criticized by Morozov (2019), who regards her theory as a limited conception of digital economy blind to systemic power relationships and what he identifies as the most central challenge of capitalism. It obscures the fact the financial motives that drive companies' data strategy and their hunt for behavioral surplus are long-term profits and competitiveness. In other words, capitalism is the root of the problem, and the collection of behavioral data is only a means to an end. Furthermore, he points out that:

> The concept of surveillance capitalism shifts the locus of the inquiry, and the struggles it informs, from the justice of relations of production and distribution inside the digitized social factory to the ethics of exchange between companies and their users. (Morozov, 2019, p. 37)

According to Morozov (2019), Zuboff gives an incomplete picture of how value is created in the digital economy by only focusing on "consumer-facing operations rather than on how organizations interact within their business and government facing operations" (p. 28). Nevertheless, Morozov acknowledges Zuboff's theory as "a strong analytical model that will inform all subsequent interpretations of the digital economy" (p. 24).

3. Journalism through the Lens of Surveillance Capitalism

In the perspective of Zuboff's surveillance capitalism, mobile journalism might be perceived, along with any other human experiences and activities, as traceable and tradeable data objects and, as such, raw material for surveillance capitalism. First, journalists and their behavior can be traced and represented as data objects along with information such as name and social networks—easily extracted from, for example, a social media profile. This includes their interactions with sources and other people, movements, and activities (Callegaro & Yang, 2018; Swan, 2013). Furthermore, these sources can be used to triangulate metadata and algorithmic analyses for developing complex profiles of individuals and their behavioral patterns (Schermer, 2011).

A recent story from the German public broadcaster NDR exemplifies the potential of using such data for identifying individual profiles and options for buying such data to target groups of people, including journalists. In an undercover action, a group of investigative journalists acquired a comprehensive data packet about the online activities of three million German citizens

over one month. The data was provided for free by a data broker, and with this information, the journalists identified and reconstructed complete work profiles of other journalists, including their movements, e-mail communication, travel schedules, and browsing activities. The data package also contained sensitive information about several German media houses, such as business strategies, sales figures, and profiles of mid-level management employees (ARD Zapp, 2016; Norddeutscher Rundfunk, 2016).

Data traded in this way is usually claimed to be anonymous, but by triangulating, for example, geo-location data with publicly available data such as addresses, the data can be de-anonymized and used to create profiles of specific people or groups of people. This also was illustrated in a case from the Norwegian public broadcaster NRK ("My phone was spying on me," 2020), where reporters investigated the dataflows and tracking activities of several Norwegian citizens based on their uses of mobile apps. The data was bought openly, and the investigation revealed a complex and invisible network of actors involved in the data analytics and data brokerage market.

While targeted surveillance, intimidation, and harassment of journalists as reprisals of their work has been occurring for many years, research on digital safety and security for journalists indicates that journalists are increasingly becoming vulnerable to attacks from state as well as non-state actors (Belair-Gagnon et al., 2016; Council of Europe, 2020; Crete-Nishihata et al., 2020; Marczak, Scott-Railton, Al-Jizawi, Anstis, & Deobert, 2020). In the last 10 years, at least 937 journalists were killed at work, according to Reporters Without Borders (2020). Many were deliberately murdered because they investigated topics such as corruption and organized crime. In the same period, an increasing number of cases demonstrate targeted uses of digital surveillance on journalists and newsrooms that put source protection and journalist safety at risk (Crete-Nishihata et al., 2020; Perlroth, 2013; Scott-Railton, Marczak, AdbulRazzak, Crete-Nishihata, & Deibert, 2017; Timberg, 2013; Wagstaff, 2014).

To understand the implications of surveillance capitalism for mobile journalism, the concept of dataveillance (Clarke, 1988; Van Dijck, 2014) can be useful. 'Dataveillance' is a form of surveillance based on mass data collection with "unstated preset purposes" (Van Dijck, 2014, p. 205) and is on the increase in many areas of society (Christl, 2014; Christl et al., 2017a; Crete-Nishihata et al., 2020; Degli Esposti, 2014; Zuboff, 2019). Dataveillance not only allows us to build profiles of individuals and their behavior, but also predicts future behavior (Schermer, 2011) and interferes in individual decision making, for example, through microtargeting (Christl, 2019).

Furthermore, trading these profiles as a commercial good gives access to sensitive information about individuals, groups of people, and organizations to a broad range of third-party actors with diverging agendas and allows its utilization for malicious purposes (Christl et al., 2017a). Christl et al. (2017a) examined and documented the massive scale and scope of unrestrained commercial exploitation of personal data that this new economic logic of behavioral data exploits. Christl et al. (2017a, p. 5) concluded in their report:

> Individuals can see only the tip of the data and profiling iceberg. Most of it occurs in the background and remains opaque; as a result, most consumers, as well as civil society, journalists, and policymakers, barely grasp the full extent and forms of corporate digital tracking and profiling.

4. Mobile Journalism as a Risk for Journalists and as a Supplier for Surveillance Capitalism

Forms of commercially motivated surveillance affect individuals and civil society (Christl, 2014; Christl et al., 2017a; Van Dijk, 2014; Zuboff, 2019). However, the risks and societal consequences related to trading behavioral data (Zuboff, 2016) are especially high for some groups. In democratic countries, journalistic institutions have invested heavily in further developing codes of ethics as responsible systems for self-regulation. Such codes of ethics complement the media regulations in various countries and are highly valued by practitioners. However, with technologies like the smartphone, journalists increasingly find themselves in a double bind of transparency; by using the smartphone as a work tool, journalists are often exposed to dataveillance themselves while contributing to the tracking of others. Christl and Spiekermann (2016, p. 47) point out that smartphones entail several specific risks regarding the privacy of users:

> The information stored on such devices, including calls, text messages, contact lists, calendars, photos, videos, visited websites, the phone's location, and motion behavior, provides detailed insights into the user's personality and everyday life. It is not only information about friends and family that is stored on such a device, but also work, finance, and health contacts. Most of the time, mobile devices are connected to the Internet. Potentially, the integrated sensors can always be activated. Many users also store passwords on their smartphone, which provide access to personal user accounts such as email, social networks, and e-commerce.

Thus, we argue that the whole process of mobile journalism can be construed as a human activity to provide raw materials and behavioral surplus for data aggregation, analysis, and algorithmic profiling and therewith open up the possibilities of behaviorally modifying journalists, such as chilling effects (Büchi et al., 2020; Eide, 2019), digital nudging (Helbing, 2019; Huang, Chen, Hong, & Wu, 2018), search engine manipulation effects (Epstein,

Robertson, Lazer, & Wilson, 2017; Helbing, 2019), doxing (Crete-Nishihata et al., 2020), and micro-targeting (Christl, 2019).

Anyone relying on technologies and infrastructures optimized for data extraction and profiling can become radically transparent for a range of actors (Christl & Spiekermann, 2016). As discussed above, journalists have always been a risk group and a main target for surveillance (Crete-Nishihata et al., 2020; Thorsen, 2019; Waters, 2018). It is well known that a range of actors in different parts of the world, such as secret services, police authorities, and other players, seek to monitor journalists' interactions and to access data stored on their computers (Henrichsen, Betz, & Lisosky, 2015). After the Snowden revelations in 2013, the mass surveillance initiated by state actors and its implications for journalism have been broadly discussed (Bradshaw, 2017; Lashmar, 2018; Mills, 2019; Waters, 2018).

While Zuboff points to the need for social action to solve the challenges arising in the wake of surveillance capitalism, she does not go to any lengths to propose how this can be addressed in practice. In our critical discussion on how mobile journalism and innovation in this field can be practiced responsibly, we will therefore take a closer look at the research and innovation policy framework RRI as a potentially complementary approach.

5. RRI as a Framework for Societal Action

To address how innovation and practice in mobile journalism can be envisioned in a responsible manner, we find the European framework of RRI to be a promising approach. The RRI approach is a normative policy strategy that acknowledges the uncertainties linked to scientific progress and socio-technological innovations and outlines ICT as a field with transformational potential for society. The RRI aims to achieve ethically acceptable, societally desirable, and sustainable outcomes of research and innovation activities (Von Schomberg, 2013). To meet these goals, RRI emphasizes the importance of public engagement and the inclusion of all relevant stakeholders throughout all stages of the innovation and research process. In this way, all stakeholders ideally become mutually responsive during the process.

From a theoretical perspective, RRI is broadly understood as a form of 'meta-responsibility' or 'higher-level responsibility' (Stahl, 2013). Owen et al. (2013) suggest that RRI is "a collective commitment to take care of the future through collective stewardship of science and innovation at present" (p. 36). RRI is conceptualized through a procedural (implemented tools and methods) and a substantial dimension (addressed values and norms). Stilgoe, Owen, and Macnaghten (2013), Owen, Macnaghten, and Stilgoe (2012) and Owen et al. (2013) suggested integrating and combining elements of reflexivity, anticipation, deliberation, and responsivity. In recent years, the concept has been expanded by the dimensions of sustainability and care (Burget, Bardone, & Pedaste, 2017). Other researchers have suggested integrating the dimensions of openness and transparency (Owen, Ladikas, & Forsberg, 2017) to ensure free and open access to relevant information. The RRI approach aims not only to inform academic research contexts but also innovation, technological development, and the adoption of technology in the private sector.

Critics of the RRI approach posit RRI is too firmly anchored in academic discussions and that it is unclear how to translate the ideas and normative principles of RRI into social realities and implement RRI tools and methods into day-to-day practices (Schuijff & Dijkstra, 2020). Other authors highlight the challenges and key problems related to governing especially ICT by pointing out that practical tools and methods of RRI often run into the fundamental uncertainty and the complex ethical challenges that are automatically linked to ICT development (Jirotka, Grimpe, Stahl, Eden, & Hartswood, 2017; Stahl, Eden, & Jirotka, 2013; Stahl, Timmermans, & Flick, 2017). Furthermore, there is little awareness about the RRI approach in the industry that manages the vast majority of innovation activities in society (Gurzawska, Mäkinen, & Brey, 2017).

6. Envisioning Responsible Practice and Innovation in Mobile Journalism

Among many journalism professionals, smartphones tend to be considered just another tool in the journalistic toolbox (Burum, 2016; Umair, 2016). Smartphones are equipped with risk technologies and include application areas such as sensor technologies, cameras, biometric sensing, ambient intelligence, and artificial intelligence. These risk technologies are specifically outlined and discussed by proponents of the RRI framework (Stahl et al., 2013, 2017). According to Zuboff (2019), the infrastructures for comprehensive data exploitation have secretly evolved based on keeping the public in the dark and the exclusion of relevant stakeholders, with little democratic legitimation. Consequently, the key technologies and the infrastructure of mobile journalism are building on what Von Schomberg (2013) called an 'irresponsible innovation' (p. 60) paving the way for what arguably can be seen in the context of mobile journalism as an *irresponsible adoption of irresponsible technology*. Although mobile technology has not been developed exclusively for journalism, journalists all over the world have adopted smartphones, exploring the boundaries of mobile technology for journalistic purposes (Salzmann et al., 2020).

Even though current surveillance infrastructures seem to present complex challenges that suggest rethinking journalistic practices thoroughly (not only for mobile journalists), a radical abandonment of smartphones in journalism appears to be an unlikely scenario, or as Christl et al. (2017a) put it: "To resist the power of this data ecosystem, opting out of pervasive tracking and profiling has essentially become synonymous with opting out of much of modern life" (p. 85). In that sense,

it is urgent for journalists, media organizations, and governments to scout sustainable and responsible solutions that might have the capacity to counterbalance these challenges.

In the following section, we outline possible implications for mobile journalism over two structural dimensions and suggest approaches that may contribute to a more responsible adoption of mobile technologies in journalism and mitigate the potential harm for journalists who use these technologies.

6.1. Implications for Mobile Journalism on an Individual Level

On an individual level, journalists can meet these challenges by taking precautionary steps to minimize involuntary, uncontrolled data extraction when using smartphones. Such steps and simple precautions are constantly taught and discussed at most journalistic conferences and gatherings. A simple first step of concern to most specialists in the field is the principle of dataflow minimization, termed *datengeiz* (data stinginess) by German-speaking privacy activists, urging journalists to develop a more conscious, critical, and cautious mindset toward their digital data routines. For example, journalists could limit the number of installed apps to a minimum and only use applications from trusted sources. It would also include trying to consciously bypass as far as possible their reliance on services, products, and infrastructures known for advanced tracking and profiling capabilities. The German journalist, activist, and scholar Moßbrucker (2019) emphasizes encrypted communication and the right to anonymity as a central task of 'journalists' digital self-defense.' He suggests that journalistic practice and technological innovations should encompass features of the 'darknet,' a collection of networks and technologies for sharing content (Biddle, England, Peinado, & Willman, 2003) attuned to privacy and anonymity that counters traceability and surveillance.

Moßbrucker (2019) argues that darknet features should become basic components of journalistic tools and could be transformed, with political and economic support, into a standard infrastructure for current communication tools. Such efforts could make the Internet in journalists' pockets safer. A growing number of journalistic websites offer adapted tools for the cyber security and digital safety of their sources. Encrypted platforms for sending files through Tor, the anonymous web browser, are widespread, as are encrypted messaging apps such as Signal or WIRE. An example is a popular platform like SecureDrop that allows secure communication between journalists and sources. It was developed by the Freedom of the Press Foundation. However, many digital defense strategies might turn out to be ad-hoc solutions. Digital tools applied by journalists to avoid surveillance do not necessarily fit well with the processes of journalism and needs of journalists (McGregor, Charters, Holliday, & Roesner, 2015). In the years ahead, even closer cooperation with journalistic support organizations, such as foundations, labs, or professional associations, might be the way to go.

Following the RRI approach, an important contribution of individual journalists to mitigate the potential harms of mobile technology and exposure to behavioral data collection would be to raise the professional and public awareness of these issues.

Nevertheless, avoiding the use of these tools can be a burden for journalists and could be seen as a chilling effect. Furthermore, there are limits to what can be done on an individual level, as journalists are largely dependent on institutional support.

6.2. Implications for Mobile Journalism on an Organizational Level

Many media organizations are competing with surveillance capitalists such as Google and Facebook. They compete for the attention of their audiences and in the market of selling ads. They are also reliant on the services of these platforms to reach their audiences, and there are complex relationships between these actors (Fanta & Dachwitz, 2020; Lindén, 2020).

Furthermore, media organizations have a long tradition when it comes to collecting and trading audience information with their advertisers. They apply a range of surveillance tools for 'editorial analytics' to optimize newsroom workflows, increase audience engagement, and attract more audiences (Carroll, 2020; Cherubini & Nielsen, 2016). According to Christl et al. (2017b, p. 17), especially big media conglomerates "are deeply embedded in today's tracking and profiling ecosystems; moreover, they have often developed or acquired data and tracking capabilities themselves" (see also Adams, 2020; Carroll, 2020; Soe, Nordberg, Guribye, & Slavkovik, 2020). Zuboff's theory can serve as an eye opener that challenges media organizations to critically reflect on the long-term implications of the digital economy, their complex entanglement with competitors like Google, and their application of data harvesting technologies such as smartphones. To approach these challenges and counteract the data exploitation of journalists, the action steps of the RRI framework could be translated into activities with a critical focus on controversial aspects of privacy, autonomy, and security issues to foster a security culture in the organization (Crete-Nishihata et al., 2020).

Legacy media could, for instance, invest more resources into regular in-house training and programs for digital self-defense to bypass infrastructures optimized for behavioral data extraction or work more closely with foundations for journalism that often have more capacity and resources to focus on developing new routines or resources for protecting journalists from data exploitation and various forms of surveillance.

Ideally, to ensure the responsible adoption of mobile technologies, media organizations could apply the RRI concept of AREA (anticipate, reflect, engage, and act)

as guidelines for action. They could work to anticipate the outcome of organizational activities and investments in mobile journalism. They could collaboratively reflect on motivations, work practices, and results of organizations' mobile engagement. They also could engage with relevant stakeholders (for example, mobile journalists, cyber security experts, media lawyers and economists, privacy and data activists, mobile technology developers, data engineers, and audience representatives) to find responsible solutions that might serve society in the best way possible. In addition, they could act according to the insights of this deliberative and multi-perspective approach. While the RRI approach probably would imply high investments in the form of time, money, and social coordination, it seems to be appropriate for understanding and bypassing extensive surveillance structures related to mobile technology in the ecosystem in which it operates.

Nonetheless, such measures would be costly. As long as media organizations operate in a highly competitive market, they might not be in a position to give such measures priority. There might also be other organizational constraints, such as a lack of managerial understanding and inflexible IT policies that can counteract a security culture (Crete-Nishihata et al., 2020).

7. Conclusion

In this article, we have reflected critically on the field of mobile journalism in light of Zuboff's theory of surveillance capitalism. For Zuboff (2019), the technological capacities for surveillance and data exploitation have metamorphosed digital infrastructures into the backbone of an emerging new and more radical form for capitalism based on the exploitation of human behavior as an unlimited raw material. Zuboff warns that this new emerging economic logic leads to the concentration of knowledge in the hands of a few, giving them an unprecedented instrumentarian power that not only threatens individual autonomy, sovereignty, and dignity but also the very foundations of democracy. We argue that, from this perspective, mobile journalism surfaces as a traceable data object where mobile journalists represent only one defined risk group that has become radically transparent to third parties. The watchdogs are not only being watched; their actions are translated into analyzable data that can be sold on markets for behavioral prediction. These issues are surfacing as increasingly complex due to the vast systems of audience surveillance conducted by media organizations themselves.

By applying the RRI framework, we outlined possible implications for mobile journalism of this double bind on an individual and organizational level. RRI guidelines would suggest engaging relevant stakeholders in deliberative discussions and critical thinking on the role of journalism in society and for democracy in light of increasing surveillance and forms of dataveillance. In the case of mobile journalism, the relevant stakeholders include journalists, media organizations, policy makers, journalism education, media researchers, and relevant foundations. A key goal would be to raise awareness of these issues between and across those stakeholders. Furthermore, regulatory frameworks that address surveillance and protect privacy of citizens is another path. In the European Union, regulatory work on e-privacy is already in the making. This work can pave the way for long-term support, both politically and financially, for the ethical design of platforms and tools for both citizens and mobile journalists. Nonetheless, this problem is not easily solved on a national level, as surveillance capitalists are multi-national corporations. In addition, as Morozov points out, the root of the problem might have to be addressed in relation to the economic system of capitalism itself.

Many of the potential harms, as pointed out in the introduction, will not be exclusive to mobile journalism, but will be the same for all citizens. As we have discussed in this article, journalists are a risk group, and the risks for society are potentially high.

Acknowledgments

This research is published as part of the ViSmedia project (The Adoption of Visual Surveillance Technologies in the News Media), funded by the Research Council of Norway under the SAMANSVAR grant program [number 247721/O81].

Conflict of Interests

The authors declare no conflict of interests.

References

Adams, P. C. (2020). Agreeing to surveillance: Digital news privacy policies. *Journalism & Mass Communication Quarterly*, *97*(4), 1–22. https://doi.org/10.1177/1077699020934197

ARD Zapp. (2016). *ZAPP*: *Nackt im Netz: Journalistenprofile im Verkauf* [ZAPP: Naked on the web: Journalist profiles for sale] [Video file]. Retrieved from https://www.youtube.com/watch?v=rY3zjNdz0lA

Belair-Gagnon, V., Agur, C., & Frisch, N. (2016). New frontiers in newsgathering: A case study of foreign correspondents using chat apps to cover political unrest. *Tow Center for Digital Journalism*. Retrieved from https://academiccommons.columbia.edu/doi/10.7916/D89W0SR5/download

Biddle, P., England, P., Peinado, M., & Willman, B. (2003). The darknet and the future of content protection. In E. Becker, W. Buhse, D. Günnewig, & N. Rump (Eds.), *Digital rights management: Technological, economic, legal and political aspects* (pp. 155–176). Redmond: Springer.

Bradshaw, P. (2017). Chilling effect. *Digital Journalism*, *5*(3), 334–352.

Büchi, M., Fosch-Villaronga, E., Lutz, C., Tamò-Larrieux, A., Velidi, S., & Viljoen, S. (2020). The chilling effects of algorithmic profiling: Mapping the issues. *Computer Law & Security Review*, *36*. https://doi.org/10.1016/j.clsr.2019.105367

Burget, M., Bardone, E., & Pedaste, M. (2017). Definitions and conceptual dimensions of responsible research and innovation: A literature review. *Science and Engineering Ethics*, *23*(1), 1–19.

Burum, I. (2016). *Democratizing journalism through mobile media: The Mojo revolution*. New York, NY: Routledge.

Burum, I., & Quinn, S. (2016). *MOJO: The mobile journalism handbook: How to make broadcast videos with an iPhone or iPad.* New York, NY and London: Focal Press.

Callegaro, M., & Yang, Y. (2018). The role of surveys in the era of "big data." In D. L. Vanndette & J. A. Krosnick (Eds.), *The Palgrave handbook of survey research* (pp. 175–192). Cham: Palgrave Macmillan.

Carroll, E. C. (2020). *News as surveillance*. SSRN. http://dx.doi.org/10.2139/ssrn.3516731

Cherubini, F., & Nielsen, R. K. (2016). *Editorial analytics: How news media are developing and using audience data and metrics.* Oxford: Reuters Institute for the Study of Journalism. Retrieved from https://ora.ox.ac.uk/objects/uuid:3e5e85d4-416d-42e6-8a58-c811ff5aa505/download_file?file_format=pdf&safe_filename=Cherubini%2Band%2BNielsen%2BEditorial%2Banalytics%2BReport.pdf&type_of_work=Report

Christl, W. (2014). *Digital tracking and corporate surveillance: Collecting, analyzing and selling personal data in the age of big data: Global trends, selected examples, risks and challenges*. Vienna: Austrian Chamber of Labour. Retrieved from https://crackedlabs.org/dl/Studie_Digitale_Ueberwachung.pdf

Christl, W. (2019). Microtargeting: Persönliche Daten als Politische Währung [Microtargeting: Personal data as political currency]. *Aus Politik und Zeitgeschichte*, *69*, 24–26.

Christl, W., Kopp, K., & Riechert, P. U. (2017a). *How companies use personal data against people: Automated disadvantage, personalized persuasion, and the societal ramifications of the commercial use of personal information* (Working Paper). Vienna: Cracked Labs Institute for Critical Digital Culture. Retrieved from https://crackedlabs.org/dl/CrackedLabs_Christl_DataAgainstPeople.pdf

Christl, W., Kopp, K., & Riechert, P. U. (2017b). *Corporate surveillance in everyday life*. Vienna: Cracked Labs Institute for Critical Digital Culture. Retrieved from https://blog.fdik.org/201710/CrackedLabs_Christl_CorporateSurveillance.pdf

Christl, W., & Spiekermann, S. (2016). *Networks of control: A report on corporate surveillance, digital tracking, big data and privacy.* Vienna: Facultas.

Clarke, R. (1988). Information technology and dataveillance. *Communications of the ACM*, *31*(5), 498–512.

Council of Europe. (2020). *Hands off press freedom: Attacks on media in Europe must not become a new normal* (2020 Annual Report). Strasbourg: Council of Europe. Retrieved from https://manueldelia.com/wp-content/uploads/2020/05/Annual-report-EN-final-23-April-2020.pdf.pdf

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

Degli Esposti, S. (2014). When big data meets dataveillance: The hidden side of analytics. *Surveillance & Society*, *12*(2). https://doi.org/10.24908/ss.v12i2.5113

Duffy, M. J. (2011). Smartphones in the Arab Spring. In M. Steffens, R. Smith, & A. McCombs (Eds.), *IPI report: Media and money* (pp. 53–56). Vienna: International Press Institute.

Eide, E. (2019). Chilling effects on free expression: Surveillance, threats and harassment. In R. Krøvel & M. Thowsen (Eds.), *Making transparency possible: An interdisciplinary dialogue* (pp. 227–261). Oslo: Cappelen Damm.

Epstein, R., Robertson, R. E., Lazer, D., & Wilson, C. (2017). Suppressing the search engine manipulation effect (SEME). *Proceedings of the ACM on Human-Computer Interaction*, *1*, 1–22.

Fanta, A., & Dachwitz, I. (2020). *Google, the media patron: How the digital giant ensnares journalism* (Working Paper No. 126). Frankfurt am Main: Otto Brenner Foundation. Retrieved from https://osf.io/preprints/socarxiv/3qbp9/download

Goggin, G. (2010). *Global mobile media*. New York, NY: Routledge.

Gurzawska, A., Mäkinen, M., & Brey, P. (2017). Implementation of responsible research and innovation (RRI) practices in industry: Providing the right incentives. *Sustainability*, *9*(10). https://doi.org/10.3390/su9101759

Helbing, D. (Ed.). (2019). *Towards digital enlightenment*. Cham: Springer International Publishing.

Henrichsen, J., Betz, M., & Lisosky, J. (2015). *Building digital safety for journalism*. Paris: UNESCO.

Huang, N., Chen, P., Hong, Y., & Wu, S. (2018). Digital nudging for online social sharing: Evidence from a randomized field experiment. In *Proceedings of the 51st Hawaii International conference on system sciences* (pp. 1483–1491). Hilton Waikoloa Village, HI: AIS eLibrary. Retrieved from https://scholarspace.manoa.hawaii.edu/bitstream/10125/50072/paper0185.pdf

Jirotka, M., Grimpe, B., Stahl, B., Eden, G., & Hartswood, M. (2017). Responsible research and innovation in the digital age. *Communications of the ACM*, *60*(5), 62–68.

Konrad Adenauer Foundation. (2020). Mobile journalism conference Asia. *Konrad Adenauer Foundation*.

Retrieved from https://mojoconference.asia

Lashmar, P. (2018). Journalistic freedom and the surveillance of journalists post-Snowden. In S. Eldridge and B. Franklin (Eds.), *The Routledge handbook of developments in digital journalism studies* (pp. 360–372). Oxford: Taylor and Francis.

Lindén, C. G. (2020). *Silicon Valley och makten över medierna* [Silicon Valley and the power over media]. Gothenburg: Nordicom.

Marczak, B., Scott-Railton, J., Al-Jizawi, N., Anstis, S., & Deobert, R. (2020 December 20). The great iPwn journalists hacked with suspected NSO group imessage 'Zero-Click' exploit. *The Citizen Lab.* Retrieved from https://citizenlab.ca/2020/12/the-great-ipwn-journalists-hacked-with-suspected-nso-group-imessage-zero-click-exploit

McGregor, S. E., Charters, P., Holliday, T., & Roesner, F. (2015). *Investigating the computer security practices and needs of journalists*. Paper presented at the 24th {USENIX} Security Symposium ({Usenix} Security 15). Retrieved from https://www.usenix.org/conference/usenixsecurity15/technical-sessions/presentation/mcgregor

Mills, A. (2019). Now you see me, now you don't: Journalists' experiences with surveillance. *Journalism Practice*, *13*(6), 690–707.

Molyneux, L. (2018). Mobile news consumption: A habit of snacking. *Digital Journalism*, *6*(5), 634–650.

Morozov, E. (2019). Capitalism's new clothes. *The Baffler*. Retrieved from https://thebaffler.com/latest/capitalisms-new-clothes-morozov

Moßbrucker, D. (2019). Überwachbare Welt: Wird das Darknet zum Mainstream digitaler Kommunikation? [World of surveillance: Will the darknet become mainstream digital communication?]. In J. Krone (Ed.), *Medienwandel kompakt 2017–2019* [Media transitions compact] (pp. 9–29). Wiesbaden: Springer.

My phone was spying on me, so I tracked down the surveillants. (2020, December 12). *NRK Beta*. Retrieved from https://nrkbeta.no/2020/12/03/my-phone-was-spying-on-me-so-i-tracked-down-the-surveillants

Nassehi, A. (2019). *Muster: Theorie der digitalen Gesellschaft* [Patterns: A theory of digital society]. Munich: Verlag CH Beck.

Norddeutscher Rundfunk. (2016, November 3). Nackt im Netz: Millionen Nutzer ausgespäht [Naked on the web: Spying on millions of users]. *Norddeutscher Rundfunk*. Retrieved from https://www.ndr.de/nachrichten/netzwelt/Nackt-im-Netz-Millionen-Nutzer-ausgespaeht,nacktimnetz100.html

Owen, R., Ladikas, M., & Forsberg, E.-M. (2017). Insights and reflections from national responsible research and innovation stakeholder workshops. *RRI-Practice*. Retrieved from https://www.rri-practice.eu/wp-content/uploads/2017/09/Experiences-from-the-RRI-national-workshops-June-2017-final.pdf

Owen, R., Macnaghten, P., & Stilgoe, J. (2012). Responsible research and innovation: From science in society to science for society, with society. *Science and Public Policy*, *39*(6), 751–760.

Owen, R., Stilgoe, J., Macnaghten, P., Gorman, M., Fisher, E., & Guston, D. (2013). A framework for responsible innovation: Responsible innovation: Managing the responsible emergence of science and innovation in society. In R. Owen, J. R. Bessant, & M. Heintz (Eds.), *Responsible innovation: Managing the responsible emergence of science and innovation in society* (pp. 27–50). London: John Wiley & Sons.

Palacios, M., Barbosa, S., da Silva, F. F., & da Cunha, R. (2016). Mobile journalism and innovation: A study on content formats of autochthonous news apps for tablets. In J. M. A. Aguado, C. Feijóo, & I. J. Marínez. (Eds.), *Emerging perspectives on the mobile content evolution* (pp. 239–262). Hershey, PA: IGI Global.

Pavlik, J. V. (2019). Advancing engaged scholarship in the media field. *Media and Communication*, *7*(1), 114–116.

Perlroth, N. (2013, January 30). Hackers in China attacked the Times for last 4 months. *The New York Times*. Retrieved from https://www.nytimes.com/2013/01/31/technology/chinese-hackers-infiltrate-new-york-times-computers.html

Perreault, G., & Stanfield, K. (2018). Mobile journalism as lifestyle journalism? *Journalism Practice*, *13*(3), 331–348.

Reporters Without Borders. (2020). World press freedom index 2020. *Reporters without Borders*. Retrieved from https://rsf.org/en/ranking_table

Salzmann, A., Guribye, F., & Gynnild, A. (2020). "We in the mojo community": Exploring a global network of mobile journalists. *Journalism Practice*. https://doi.org/10.1080/17512786.2020.1742772

Schermer, B. W. (2011). The limits of privacy in automated profiling and data mining. *Computer Law & Security Review*, *27*(1), 45–52.

Schuijff, M., & Dijkstra, A. M. (2020). Practices of responsible research and innovation: A review. *Science and Engineering Ethics*, *26*, 1–42.

Scott-Railton, J., Marczak, B., AdbulRazzak, B., Crete-Nishihata, M., & Deibert, R. (2017, June 19). Reckless exploit: Mexican journalists, lawyers, and a child targeted with NSO spyware. *Citizen Lab*. Retrieved from https://citizenlab.ca/2017/06/reckless-exploit-mexico-nso

Soe, T. H., Nordberg, O. E., Guribye, F., & Slavkovik, M. (2020). Circumvention by design-dark patterns in cookie consent for online news outlets. In *Proceedings of the 11th nordic conference on human-computer interaction: Shaping experiences, shaping society* (pp. 1–12). New York, NY: ACM.

Stahl, B. C. (2013). Responsible research and innovation: The role of privacy in an emerging framework. *Science and Public Policy*, *40*(6), 708–716.

Stahl, B. C., Eden, G., & Jirotka, M. (2013). Responsible

research and innovation in information and communication technology: Identifying and engaging with the ethical implications of ICTs. In R. Owen, J. R. Bessant, & M. Heintz (Eds.), *Responsible innovation: Managing the responsible emergence of science and innovation in society* (pp. 199–218). London: John Wiley & Sons.

Stahl, B. C., Timmermans, J., & Flick, C. (2017). Ethics of emerging information and communication technologies. On the implementation of responsible research and innovation. *Science and Public Policy*, *44*(3), 369–381.

Stilgoe, J., Owen, R., & Macnaghten, P. (2013). Developing a framework for responsible innovation. *Research Policy*, *42*(9), 1568–1580.

Swan, M. (2013). The quantified self: Fundamental disruption in big data science and biological discovery. *Big Data*, *1*(2), 85–99.

Thorsen, E. (2019). Surveillance of journalists/encryption issues. *The International Encyclopedia of Journalism Studies*. https://doi.org/10.1002/9781118841570.iejs0272

Timberg, C. (2013, December 18). Hackers break into Washington Post servers. *The Washington Post*. Retrieved from https://www.washingtonpost.com/business/technology/hackers-break-into-washington-post-servers/2013/12/18/dff8c362-682c-11e3-8b5b-a77187b716a3_story.html

Umair, S. (2016). Mobile reporting and journalism for media trends, news transmission, and its authenticity. *Journal of Mass Communication & Journalism*, *6*(9), 323–328.

Van Dijck, J. (2014). Datafication, dataism and dataveillance: Big data between scientific paradigm and ideology. *Surveillance & Society*, *12*(2), 197–208.

Von Schomberg, R. (2013). A vision of responsible research and innovation: Responsible innovation: Managing the responsible emergence of science and innovation in society. In R. Owen, J. R. Bessant, & M. Heintz (Eds.), *Responsible innovation: Managing the responsible emergence of science and innovation in society* (pp. 51–74). London: John Wiley & Sons.

Wagstaff, J. (2014, March 28). Journalists, media under attack from hackers: Google researchers. *Reuters*. Retrieved from https://www.reuters.com/article/us-media-cybercrime-idUSBREA2R0EU20140328

Waters, S. (2018). The effects of mass surveillance on journalists' relations with confidential sources: A constant comparative study. *Digital Journalism*, *6*(10), 1294–1313.

Westlund, O., & Quinn, S. (2018). *Mobile journalism and MoJos*. Oxford: Oxford University Press.

Zuboff, S. (1988). *In the age of the smart machine: The future of work and power.* New York, NY: Basic Books.

Zuboff, S. (2015). Big other: Surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology*, *30*(1), 75–89.

Zuboff, S. (2016, March 5). The secrets of surveillance capitalism. *Frankfurter Allgemeine Zeitung*. Retrieved from https://www.faz.net/aktuell/feuilleton/debatten/the-digital-debate/shoshana-zuboff-secrets-of-surveillance-capitalism-14103616.html

Zuboff, S. (2019). *The age of surveillance capitalism: The fighting for a human future at the new frontier of power*. New York, NY: Public Affairs.

Zuboff, S. (2020, July 29). The case for breaking up tech empires. *CNN News.* Retrieved from https://edition.cnn.com/videos/tv/2020/07/29/tim-bray-shoshana-zuboff-big-tech-antitrust-aman

About the Authors

Anja Salzmann is a PhD Student at the Department of Information Science and Media Studies at the University of Bergen, Norway. She is part of the transdisciplinary Vismedia project and network that has investigated the adoption of visual surveillance technologies in the news media. Her research interests include journalism innovation, digital infrastructures, surveillance and dataveillance technologies, information economy and critical theory. ORCID: https://orcid.org/0000-0001-7447-5410

Frode Guribye is a Professor of Information Science at the Department of Information Science and Media Studies, University of Bergen, Norway. He focuses on human–computer interaction and the social implications of ICTs. His research spans different application areas such as technology-enhanced learning, computing and mental health, and mobile journalism. Across these areas, he is doing research through design and empirical studies aiming to critically and constructively understand the potential and limitations of emerging technologies. ORCID: https://orcid.org/0000-0002-3055-6515

Astrid Gynnild is a Professor of Media Studies at the Department of Information Science and Media Studies, University of Bergen, Norway. She is Head of the Journalism Research Group and Principal Investigator of the ViSmedia project. Her current research focuses on surveillance prospects of journalism innovation and emerging technologies. ORCID: https://orcid.org/0000-0002-9502-1044