Check for updates

*Original Research Article*

BIG DATA & SOCIETY

Big Data & Society
July–December 2016: 1–11
© The Author(s) 2016
DOI: 10.1177/2053951716669381
bds.sagepub.com
SAGE

# Reluctant activists? The impact of legislative and structural attempts of surveillance on investigative journalism

**Anthony Mills and Katharine Sarikakis**

**Abstract**

If we accept that surveillance by the State and 'sousveillance' by the media in Western democracies tend towards a relative equilibrium, or 'equiveillance' supported by the function of journalism as a watchdog and that the rule of law largely protects fundamental freedoms, this paper argues that the act of 'mutual watching' is undesired by the State and comes at a very high cost to journalists. The combination of technological capacity, legislative change and antidemocratic sentiments of the State, in the context of its willingness and ability to collect and process Big Data on an unprecedented scale, disrupt the preconditions for a strong democracy based on free media and free citizens. This paper examines the politics of investigative journalism under the conditions of dominance of the State by investigating the experiences of journalists with surveillance. Our interviews with 48 journalists show that journalists are acutely aware of surveillance and its noxious impact. Well beyond simple 'watching' these experiences are remarkably similar in non-Western and Western countries. Journalists are engaging increasingly with technological and other communities, as they aim to defend journalism and their lives. Their activism is operationalised in three areas: (a) in reluctant often-fraught cooperation with hacktivists, (b) in self-directed protection of communications and sources and (c) in not always willingly acting as dissenters vis-a-vis the State. This paper explores the extent to which journalists consider equilibrium to be distorted, and how they are countering any slide into subdued democracy.

**Keywords**

Surveillance, journalism, activism, freedom of information, law, press freedom

## Surveillance and journalism

One of the documents released by Edward Snowden in 2013, destined for army intelligence, warned that 'journalists and reporters representing all types of news media represent a potential threat to security', adding: 'Of specific concern are ''investigative journalists'' who specialise in defence-related exposés either for profit or what they deem to be of the public interest' (The Guardian, 2015a). This put in no uncertain terms journalists as specific targets in a 'surveillance web' (Lyon, 2015: 24). While the surveillance of journalists predates the modern surveillance society era, the already-existing zealous willingness of State actors, coupled with an unprecedented technological ability to gather and analyse huge amounts of digital information, or Big Data, represents an unparalleled threat to watchdog journalists and their confidential sources, including whistle-blowers, even in Western democracies. In the current surveillance state climate, investigative journalists are faced with the exponentially growing challenge of securing (1) their communication with each other, (2) their communication with sources and (3) the sometimes-huge volumes of top-secret Big Data *they* store and analyse to produce public interest journalism.

In 2009 Dover and Goodman noted that sustained academic analysis of the broader relationship between

Department of Communication, University of Vienna, Vienna, Austria

**Corresponding author:**
Katharine Sarikakis, Department of Communication, University of Vienna, Währinger Straße 29, 1090 Vienna, Austria.
Email: katharine.sarikakis@univie.ac.at

Creative Commons CC-BY: This article is distributed under the terms of the Creative Commons Attribution 3.0 License (http://www.creativecommons.org/licenses/by/3.0/) which permits any use, reproduction and distribution of the work without further permission provided the original work is attributed as specified on the SAGE and Open Access pages (https://us.sagepub.com/en-us/nam/open-access-at-sage).

the media and intelligence agencies has been thin. Existing studies on agenda-building efforts by Western intelligence agencies adopt a broader view of the ways in which the government, the media, and citizens influence each other's agendas (Bakir, 2013; Lang and Lang, 1981).

A mutually influencing dynamic is established through leaks and official inquiries, news media using technology and live dissemination capacities, and NGOs representing civil society. However, the State's strategic actions include spying on the media (Alwood, 2007), harassing and blacklisting journalists (Spaulding, 2009).

Spaulding observes that in climates involving the targeting of dissent by the authorities, constitutional rights are far from a guarantee against targeting and blacklisting, and the curtailment of freedom of speech, even for journalists. Not only 'backward' democracies or repressive regimes, but also Western democracies engage actively in covert surveillance of journalists.

Andrejevic (2006) called post 11 September state surveillance asymmetric amid a constant push by state intelligence bodies to enhance their technological surveillance capabilities, while at the same time intensifying the secrecy within which they operate. He notes that although the news media have reported on this asymmetry, their doing so cannot be considered 'reciprocal' surveillance because for the most part it amounts to underscoring 'just how little we know about the government's use of new media technology to accumulate, store, and sort information about citizens' (Andrejevic, 2006: 395). Troublingly in the view of Campbell and Carlson (2002), subjects willingly participate in their own surveillance, possibly due to a commodification of privacy, in which its value as a human right is no longer recognised but it is willingly compromised in return for consumer benefits. Furthermore, the possibility of opting out of such bartered-away privacy and self-facilitation of consumer surveillance may in most instances be illusory (Elmer, 2003). There is nonetheless a growing willingness to organise monitoring of, and resistance to, what Fernback (2013) calls networked surveillance by actors such as Facebook. 'These actions are an attempt at equality and responsibility in a democratic society that disrupts the institutionalized power of panoptic surveillance' (Fernback, 2013: 19).

'Sousveillance' or 'surveillance from below' (Fernback, 2013; Ganascia, 2010; Mann and Ferenbok, 2013) and its interplay with the media and politico-strategic communication has evolved rapidly (Bakir, 2010), tending – at least in Western democracies – towards a form of equiveillance (Mann et al., 2006), an uneasy constantly threatened balance between the surveillors and the surveilled, who make use of easily accessible rapidly evolving citizen media surveillance technology. Sousveillance has been facilitated through the variegation and innovation of news production networks and platforms, as well as through the increased emergence of social media and whistleblowing sites (Bakir, 2015). Ganascia (2010) highlights the fact that developments in sousveillance technology have fused the hitherto more separate realms of private and public sphere.

The ways in which surveillance developments relate *specifically* to journalism and in particular investigative journalism in its watchdog role is an understudied area. There is little known in academic work on the effects of attempts at 'mutual watching' that digital whistleblowers and WikiLeaks engage in, for journalism as a watchdog. An examination of the ways in which news media are reacting to counter the effects of such surveillance, legislation and efforts at manipulation or how they might seek equiveillance, as described by Mann et al. (2006), is also necessary. Even how journalists are using advances in technology, such as encryption and other secure forms of communication, and means of countering surveillance is rather under-researched. Mann et al. (2003) describe, in more general terms, the turning against, or 'detournement' of surveillance techniques, by the surveilled against the surveillors as reflectionism, but do not make the case specifically for journalists. Bakir (2015) highlights this paucity of research, noting that only a fraction of academic journal articles deal with the interplay between intelligence agencies' agenda-setting and journalism. Bakir explores the ways in which mass surveillance impacts on the democratic process and the media, including the erosion of the watchdog role of the media, and the weakening of democracy as a whole, particularly in conjunction with other restrictive legislation linked to national security (Bakir, 2015).

Following the outline of relevant, limited, scholarship and after a description of methodological concerns, this paper reports on the findings deriving from in depth interviews with journalists with regard to these under-studied questions. In this vein, this research is problem-driven but with the aim to provide impetus towards further theoretical development and analysis of the factors shaping communicative environments within which a 'watchdog' philosophy of investigative journalism is crucial for democracy.

## Methodology

Problem-driven research begins with a diagnosis and evidence of a particular difficulty impeding a social relation. In this case, the issue at stake is the degree to which journalism as the so-called fourth estate may be dis/enabled to fulfil its function, and whether media governance within democratic environments enables a watchdog journalism in the age of surveillance marked

by unprecedented Big Data retention capacities, in terms both of legislation and technology. Problem-driven research is associated with solution-aimed research. This is often the case, although solution must not be assumed to be a prescription for concrete practices necessarily. We apply a non-reductionist critical approach to understand and map the array of influences experienced in the everyday practice of journalism, when it involves the investigation of uncomfortable questions and sensitive issues. We do so, by taking as our departing point the well-documented fears of and criticisms against the capacity and practice of mass surveillance over citizens and journalists. The treatment of whistle-blowers, such as Julian Assange, Edward Snowden, Chelsea Manning, and Antoine Deltour and Raphael Halet, of LuxLeaks (Reuters, 2016a, 2016b; The Guardian, 2015b, 2016a), as front people of the freedom of information movement, by the State has been punitive. We gathered evidence in three stages: the first stage is the identification of possible impediments to freedom of imparting information due to surveillance. Existing academic and other writings and reports allowed us to identify an array of possibilities of interference as well as counteraction. Second, we identified journalists who fulfil the following characteristics: they are known for their investigative work; have 10 years' experience in the field or more; engage in international topics; work with major media companies. We aimed to ensure and capture experience and knowledge in investigative journalism of a 'before' and 'after' picture of surveillance. Almost all of our subjects are also either staff members of, or have close ties to, major media companies, and/or stable employment conditions to the degree that these are achievable under the financial crisis, hence they can rely on the relative security necessary to pursue investigative work. We interviewed 51 individuals, 42 of whom are journalists (US: 7; Germany: 5; Austria: 5; Hungary: 3; UK: 3; Greece 4; Turkey: 3; France: 2; Morocco: 1; Netherlands: 1; Syria: 1; Lebanon: 1; Russia: 1; Iran: 1; Egypt: 1; Italy: 1; Zimbabwe: 1; Poland: 1), working in print, broadcast and online. We interviewed eight media experts, including former journalists, active in media research/advocacy for NGOs and a university (Poland: 3; Hungary: 2; UK: 1; US: 1; Serbia: 1). Two of the journalists we interviewed also have experience of media advocacy for an NGO. Finally, we also interviewed one whistle-blower. The selection of interviewees was a combination of accessibility and an effort to include journalists based in countries with varying degrees of freedom. The countries referred to span rankings in the Reporters without Borders (2016) World Press Freedom Index from 2 (The Netherlands) to 177 (Syria), and scoring from 11 (The Netherlands) to 90 (Iran) on the 'Freedom of the Press 2016' index (Freedom House, 2016).

We ceased to conduct interviews when we reached saturation of responses. Our aim was to explore the views and strategies of journalists in the current climate of mass surveillance, whether effective or not, and in relation to the future of journalism. Interviews lasted between 15 minutes and two hours and took place not only in private or public physical spaces, but also online and by phone. In some cases, interview appointments were arranged without electronic means and/or on some occasions mobile telephones were not present, i.e. carried by the researchers or the interviewee. We used online technology that is argued to provide some basic protection of privacy. Our data analysis is based on inductively identifying themes as they emerged from the discussions with journalists. Interviews were semi-structured with the aim to allow professionals themselves to identify core issues with surveillance and to speak of coping and their tactics of resistance. We aimed at addressing a comprehensive universe of factors from technology to media organisation, and from personal views to professional judgements with regard to the profession and democracy. Hence we followed ground theory practices to allow the data to speak for itself, but starting from the basic categories of enquiry. Further, we sought to identify patterns, connections and divergence among the responses and connect those back to the political, economic and institutional dimensions of the journalistic environment(s). Here, we use only those names and quotes for which we were given permission but also draw upon information given by the anonymised subjects.

## Legislative pressure

In recent years, the immediate aftermath of terror attacks in the USA in 2001 and later in Madrid, London, Paris and Brussels have brought about a public discourse ready to compromise on fundamental rights in the name of security, enhanced through new legislation that has enshrined in law the right of State actors to gather and analyse enormous amounts of communications data. The Patriot Act, passed just six weeks after 11 September, facilitated spying on ordinary American citizens through surveillance of phone and email communication, of bank and credit card records, and of Internet activity (American Civil Liberties Union, 2016). Lyon (2003) noted that 'responses to 9/11 are serving to speed up and spread out such surveillance in ways that bode ill for democracy, personal liberties, social trust and mutual care' (p. 6). The Snowden revelations in 2013 subsequently showed the degree to which secretive mass surveillance of huge numbers of innocent American citizens had been conducted by the NSA for years, including the systematic gathering of phone records of tens of

millions of people, and the routine, direct tapping into the servers of nine US Internet companies including Google, Facebook and Microsoft (BBC, 2014). Meanwhile, the Foreign Intelligence Surveillance court, tasked with approving requests for surveillance of a foreign subject, in which the communications of US citizens may be caught up, meets in secret (The Guardian, 2015c).

Metadata surveillance coupled with unprecedented technological surveillance analysis capacities make it far easier to identify journalists' sources. Maybe that is the reason why under the administration of US President Barack Obama, there have already been more prosecutions of whistle-blowers and leakers than under all previous presidential administrations combined (Foreign Policy, 2013).

A series of legislative changes across mature democracies aim to cement and normalise the state of surveillance over communication by assigning such powers to a range of institutions and without the necessary oversight of the judicial system. In a 2015 report, the Council of Europe's commissioner for human rights, Nils Muižnieks, noted that democratic oversight of national security services in Europe remains 'largely ineffective' (Council of Europe, 2015a). In the US, in May 2016, it emerged during a Senate Judiciary Committee hearing that government representatives did not know how many Americans have been affected by a secretive surveillance programme (Electronic Frontier Foundation, 2016).

The common threads of these laws are the enlargement of the State and the restriction of individuals through increased mass surveillance; gathering of monitoring data; restrictions to information dissemination for journalists and citizens. We are currently witnessing the fundamental and gradual redrafting of fundamental freedoms, such as privacy and the freedom to access and impart information.

In the UK, the proposed Investigatory Powers Bill allows for increased, disproportionate surveillance by police, security services and other state entities without sufficient oversight (The Guardian, 2016b). Opposition politicians, journalists and human rights observers have warned that the proposed Bill threatens journalistic secrecy.

In Germany, treason legislation has recently been used against journalists who divulged national security information provided by a confidential source. Spain's new Citizens Security Law, also referred to as the gagging law, outlaws 'the unauthorised use of images of police officers that might jeopardise their or their family's safety or that of protected facilities or police operations' (The Guardian, 2015d).

In France, surveillance law no. 2015-912 of 24 July 2015 grants powers to the security services to monitor the phone and Internet activity of anyone suspected of links to terrorism, without the need for judicial approval (Re/code, 2015). In addition, the law requires Internet companies to install 'black boxes' that suck up, for analysis, metadata of huge numbers of Internet users in France. A flexible definition of 'link to terrorism' could see the communication of journalists directly targeted.

Draft legislation for new Dutch surveillance laws provides security services with broad powers to intercept Internet data, in a move the Dutch Human Rights Commission branded 'a major infringement of the right to privacy and secret communications' (Irish Times, 2016). Hungary's 2011 anti-terror surveillance legislation, meanwhile, was found in early 2016 by the European Court of Human Rights to be a violation of European privacy law.

In Poland new surveillance legislation, in particular increased intelligence agency access to data, and a loosening of controls on police surveillance are central to fears about a broad slide towards illiberal democracy reminiscent of that in Hungary (Reuters, 2016c).

Across the world, surveillance legislation is being drafted in the name of combating terrorism and enhancing security (Council of Europe, 2015b). A core common threat of all such legislation is the increased space, with insufficient transparency and oversight, for State actors to disproportionately gather and analyse communications data of citizens. The authority of national citizens is being potentially eroded, through a reconfiguration of the notions of privacy, secrecy, communication and even democracy, by a 'new nobility of intelligence agencies operating in an increasingly autonomous transnational arena' (Bauman et al., 2014: 126). This new nobility is unlikely to see its primary objective as the securing of democracy regardless of what politicians may say: 'the old suspicion that agencies claiming to secure our life and well-being often turn out to be extremely dangerous retains considerable wisdom' (Bauman et al., 2014: 134). Bauman et al. (2014) argue that Western democracies are not (yet) on the verge of totalitarianism, but the focus on more intrusive, widespread surveillance and invasions of privacy in the name of security constitute a threat of the kind seen in undemocratic states to entrenched liberties – among them the right of a free press to hold public officials, including those who operate intelligence agencies, to account. This reconfiguration, which security agencies highlight in particular after terrorist attacks, elevates 'security' as a primary concern. 'What used to be understood as authoritarian options are made to seem desirable, even natural' (Bauman et al., 2014: 137).

## The experiences of surveillance

In Western democracies, which now constitute a 'surveillance society' (Lyon, 2015: 28), journalists tend not

to face the same kind of physical risks as those in repressive regimes, but the aim and *act* of intimidation through surveillance is a commonality with non-Western countries. Our interviewees listed frequent undue delays and harassment when travelling through airports; threat of prosecution under secrecy, treason or espionage laws; physical or online intrusion, signalling the presence of surveillance and the disregard of rights to freedom of movement, to information, privacy and dignity.

### *Inhibiting freedom of movement*

For months after he interviewed Snowden in Hong Kong, Guardian journalist Ewan MacAskill (interview, 2 March 2016) was pulled out of the passport line every time he left the UK through Heathrow airport: 'They would say, ''Your passport's been lost.'' I said, ''Well, it's not lost, I haven't reported it lost.'' And then next time: ''Your passport's been stolen.'' I said, ''It's not been stolen''... Every time it was a different reason.' Then-Guardian journalist James Ball (now with Buzzfeed News UK) (interview, 2 March 2016), who was also on the Snowden reporting team, had 'constant aggravation' entering the US in the months after the Snowden story broke: 'Every time I flew through I would get a full bag search and then secondary security screening.

Italian journalist Stefania Maurizi (interview, 12 March 2016), who covered both WikiLeaks and Snowden for the Italian weekly L'Espresso, was harassed while transiting an airport [in Italy], where she was singled out for secondary screening after being paged on the airport loudspeaker system.

'People who have decided to work in this field know that the next time they go to the States it can happen that they are thoroughly searched and that all their electronic devices will be taken... and so on. And this could also happen in London Heathrow,' says Michael Sontheimer (interview, 15 March 2016), who coordinated Der Spiegel's Snowden coverage.

### *Deliberate intrusion and surveillance signalling*

Unmarked vans were parked outside the homes of journalists who covered the Snowden story (Luke Harding, interview, 29 February 2016). The Guardian was forced to destroy the hard drives of computers used in its reporting with pneumatic drills and sledge hammers in the basement under the watch of two note- and photograph-taking security officials from The Government Communications Headquarters (GCHQ) – one of whom allegedly said: 'We can call off the helicopters' (Reuters, 2013). Luke Harding, who was also on the Guardian's Snowden reporting team, says the computer destruction incident 'was Stasi, because... what democratic government forces a national newspaper to destroy their computers?'

He recalls as well: 'There were trucks that would roll up outside The Guardian's offices and outside her (then-Guardian US editor Janine Gibson) home. I had some strange encounters in Rio... when I met Glenn (Greenwald) we had to move location about three or four times because suddenly a whole host of people were kind of eavesdropping on us... These unpromising young men would suddenly sit with their backs to us. Subsequently I was more or less propositioned by someone who looked like CIA central casting in the lobby of my hotel, a guy... suggesting we should go sightseeing together.'

A month later, when Harding was writing his book about the Snowden affair, the noticeable surveillance took a bizarre turn: 'At certain points in the text... someone would start remotely deleting the text.'

Maurizi was also targeted with 'aggressive', intimidating overt physical surveillance during the Snowden coverage, in a public park where she was meeting a high-level source in the late afternoon in Berlin. And Sontheimer says: 'One of our colleagues was followed by quite a few agents of a secret service.'

Luke Harding from the Guardian recalls the covert surveillance as he and his colleagues reported on Snowden: 'Janine Gibson [then-US-editor of The Guardian], her chats with Glenn Greenwald kept on falling through, there was someone trying to get a ''man in the middle'' [interception hack] on her laptop.' 'If you work in this field you can be sure that your phone numbers, your email address and so on will end up on some selectors list of the NSA or GCHQ,' adds Sontheimer from Der Spiegel, which learned from the Snowden leaks that half a year after it covered the WikiLeaks cables in 2010, its research was monitored and phone calls surveilled (Holger Stark, interview, 15 March 2016).

Journalists interviewed for this paper who were subjected to this kind of surveillance reported adopting a variety of digital counter-security measures. Nonetheless, so advanced and pervasive are the surveillance capabilities of certain States that it is becoming increasingly difficult for journalists who work on sensitive stories to find any 'safe space' at all. Many of them reported feelings of 'paranoia'.

### *Threat of legal action*

Journalists at the Guardian newspaper in the UK knew that if they did not comply with certain demands their newspaper could be shut down. 'You've had your fun,' they were told by the government. 'Now we want the stuff back (The Guardian, 2013).' The Official Secrets Act was mentioned. Ewan MacAskill was 'prepared by

Guardian lawyers for going in front of a grand jury' when he flew to the Guardian's offices in New York. More than two years on, UK journalists who covered Snowden are still 'under investigation'.

A criminal treason investigation, carrying the threat of lengthy imprisonment was opened in Germany against Markus Beckedahl, the founding editor of German data and surveillance news website Netzpolitik (interview, 12 March 2016) and a colleague of his after they published an article based on confidential documents from the BND, Germany's federal intelligence agency. As soon as he was officially named a suspect in a treason investigation, the intelligence agencies were legally allowed to mobilise surveillance tactics under the 'anti-terror' umbrella. 'That's something we were until now familiar with from repressive regimes,' says Beckedahl.

### *Chilling effect*

US investigative journalist Seymour Hersh (interview 16 March 2016) says: 'The government's always hostile to reporters that tell a different story than they do. It's always been chilling.' But he notes that they 'now have more tools they can use'.

The enhanced surveillance capacities and the willingness to deploy them on a massive, intrusive scale in Western democracies are having a 'great impact' on watchdog journalism, warns long-time US national security reporter James Bamford (interview, 24 March 2016) 'I think it is the beginning of what might be called a Panoptic society.'

The emergence of the surveillance state in Western democracies has chilling effect implications far beyond the realm of journalism, Maurizi warns: 'I have serious concern not only for me and my profession . . . but for everyone.'

Maurizi is echoed by Beckedahl, from Netzpolitik: 'Of course we are more hesitant to get on the phone with certain sources. We minimise email contact, even when it's encrypted . . . The kind of surveillance systems we have set up after 9/11 would have been a dream for the East German Stasi [secret police].'

'Western democracies are democracies until you do something, you step out of the cosy circle of accepted appropriate ''information''' states US investigative journalist Gavin MacFadyen (interview, 16 March 2016).

Alan Rusbridger (interview, 25 April 2016), editor of *The Guardian when it broke the Snowden story*, warns: 'If you believe that the role of journalism is to hold people to account, to provide verifiable information, so that people know what's actually going on, that someone's going to challenge the official version of events . . . the more you inhibit that, the more you damage democracy.'

## Surveillance of journalists in eroded and non-Western democracies

When increasingly pervasive, technologically advanced and unaccountable surveillance is combined with erosions of other democratic ingredients such as judicial and media independence, the Panoptic chilling effect of ubiquitous surveillance is intensified for journalists and their sources.

'I am fully aware that my emails, my phone calls, are monitored,' says Hungarian investigative journalist Attila Batorfy (interview, 21 January 2016). He refers to a colleague who investigates espionage stories, being threatened: 'The secret police was very clear: stop writing articles about our job [or] we will publish your conversations, your emails, your family background, on government-linked sites.'

Prominent Hungarian investigative journalist Attila Mong (interview, 03 February 2016) warns of a 'grey zone' around the secret services and police involving contractors and subcontractors. 'They don't ask for the special permission from a judge described in the legislation. They just do it.'

Polish investigative journalist Makarenko (interview, 24 February 2016) says that there is concern within the journalistic community in Poland about new legislation making surveillance 'out of control'. He says: 'They don't need a court order to eavesdrop or monitor my activity online whatsoever.'

In Turkey, Sevgi Akarcesme (interview, 23 March 2016), editor-in-chief of Turkey's *Today's Zaman* newspaper until it was taken over by the government, says: 'When you know you are being monitored by Big Brother you watch your words.'

The further a country moves across the political spectrum away from democratic standards, the greater the frequency with which surveillance of critical journalists is linked to the threat of, or actual, physical harm, including assassination, when the surveillance fails to have its intended chilling effect.

Lebanese journalist Samir Kassir, husband of BBC Arabic journalist Gisele Khoury (interview, 24 February 2016), was killed by a car bomb in Beirut in 2005. 'In 2001 we [my husband and I] knew we were under surveillance. They wanted to make it obvious. When we were in restaurants they were at the table near us, they followed our car, they tried one night to be very close to his body when we were walking.'

Among the many journalists detained in Syria was Beirut-based freelance reporter Sofia Amara (interview 25 January 2016), who was held at Damascus airport. 'They had my name at the airport. As soon as I stood there I thought, I'm dead . . . It was the longest two or three hours of my life.'

A common characteristic of surveillance of journalists under repressive regimes is the deliberately overt nature of elements of the surveillance, to maximise the chilling effect.

'Security agents make no secret of the fact that they are monitoring Facebook and Twitter accounts,' says Egyptian journalist Shahira Amin (interview, 28 February 2016), who adds: 'My phones are tapped and a security official has told me that I'm being monitored.'

A journalist who has worked in Iran, and was imprisoned there because of that work (interview 04 March 2016) recalls: 'I remember I was in a park with one of my friends, and he said, Hey, look over there, there's a woman in a chador filming us,' recalls 'And then when I was imprisoned and interrogated they asked if I knew they had been following me.'

## In rush to resist surveillance and protect sources, journalists take the cryptography crash course

Resistance to surveillance today involves technology-geared tactics: taking crash courses in encryption, digital tech and cyber security in general, irrespective of the 'level' of democracy. The operational security measures now used range from 'burner' throwaway mobile phones, which are more difficult to monitor, to the deliberate destruction of email correspondence so that it cannot be used in possible future legal proceedings or to identify secret sources, to an emphasis on face-to-face meetings with confidential sources, to eschewing electronic communication and its associated surveillance risks entirely, and to the setting up of both online and physical dead drop boxes, like that of The Guardian in New York.

Journalists are also much more cautious now about cross-border travel with data and what their email trail indicates. 'I'd definitely be careful about not carrying, especially across a border, some material that contains the names of sources who were confidential who I thought might get in trouble and I've become much more careful about what I put in emails, that's for sure,' says *New York Times* national security reporter Scott Shane (interview 18 March 2016). 'Because the emails that I exchanged with John Kiriakou that turned up in that prosecution I thought of at the time, and I think of today, as completely innocent and not revealing any kind of criminal action on his part. That's not the way the Justice Department ended up seeing it.'

Journalists engage in intensified operational security, including encryption of hard disks, chat, messaging and email using apps like Signal, Red Phone, or Proton Mail and PGP public (communications encryption) keys, use of the anonymous Tor (browser), password security optimisation including two-step verification, use of air-gapped computers (that are never connected to the Internet) 'We just endlessly take precautions now,' says MacAskill. His colleague at the Guardian, Luke Harding (interview, 29 February 2016) says: 'For the first six months after Snowden, when I was meeting the editor and the rest of the staff, the first thing we'd do, we'd get rid of our IPhones. We'd lock them away or put them in a different part of the building' or 'in the fridge [which interferes with audio interception and surveillance]... I don't have it around whenever I'm having a semi-serious conversation.' Mediapart editor Edwy Plenel (interview, 16 March 2016) puts no diary appointments or any other important information online. Instead he uses small notebooks, which he subsequently destroys.

In Zimbabwe, investigative reporter Tawanda Kanhema (interview, 06 December 2015) says, the cat-and-mouse surveillance game with the authorities has even more facets: 'They tell you you can't take pictures so you have to come up with ways of protecting your physical data storage devices. You have to come up with ways of protecting your computer physically beginning from guarding against burglaries into your apartment by people, by third-party actors affiliated with the state. You have to take that first step of ensuring that you don't store any data on physical storage devices that are kept in your home.'

There is also the challenge of securing data, not just communications. Polish investigative journalist Makarenko says: 'Everything we collect needs to be secured, and so far this is not the case. More and more sensitive data will be moved to the cloud. The question is who is going to manage the cloud.'

There's a flip side to using digital security, though, especially in undemocratic countries like Russia. Russian journalist Andrei Soldatov (interview 29 February 2016) warns that if journalists start using encryption, that really gets the Federal Security Service interested in them because they feel that they must have something suspicious to hide. But there's another aspect for journalists where the danger of physical harm for journalists is high: 'Imagine you have your laptop locked, encrypted with all the latest cutting-edge technologies... you cross the border and you might be stopped by border troops at the airport or some other border control point, and you might be asked to open your laptop. At that point you might compromise in order to be let in or not to miss your flight.' Another possibility, says Soldatov, is that 'you are stopped with your encrypted laptop in a conflict zone. This happened to a journalist for Novaya Gazeta who was stopped by separatists and put in jail and he was ''kindly'' asked to provide the password or they would ''break all his fingers...''. Sometimes the

best encryption is to not bring your laptop with you at all or to have a blank laptop with no emails, no photographs, just a basic device, that's all.'

Veteran UK investigative journalist Duncan Campbell (interview, 15 March 2016), too, warns that investigative journalists should not fall into the trap of relying entirely on the security offered by digital security: 'Forget all the magic crypto-stuff . . . Secure Drop and all of the other new-fangled stuff is of no use at all if the metadata that [the sources] may have left in numerous places which identifies their exploratory journey or contemplation of ethical issues can be found . . . You have a stack of burner phones and a plan . . . so that you do not go for the tecchie solution . . . but as soon as possible, and as untraceably as possible you break the metadata trail and you have to get to human contact with that person.' And if you're meeting a source, 'don't take your phone.'

In some instances, surveillance may not have the intended effect of completely subduing journalists, prompting a degree of anger and stubborn determination to 'resist'. White and Zimbardo (1980: 51) used the term 'reactance' to describe a condition in which 'people will be upset at their loss of freedom, will increase efforts to exercise their free speech, and may attack the agents of the surveillance.' Such 'reactance' lies at the heart of Lyon's assertion (2015) that there *is* hope for a fightback against the surveillance state.

## An emerging nexus? Traditionally reluctant to embrace 'activism', journalists join forces with hacktivists to fight back

In the age of social media, in which the ability to record and disseminate information lies at virtually everybody's fingertips, the line between journalism and activism is in many instances becoming increasingly blurred (NiemanReports, 2014), unnerving many traditional journalists who consider activism to be entirely separate from journalism. Many journalists would agree with the view of Guardian columnist and digital media professor Dan Gilmor who argues that professional journalists should be: thorough; accurate; fair; independent (not in terms of being free of the inherent biases of employers and one's self, but in the sense of being willing to challenge assumptions) (onMedia, 2014). And they would subscribe to the view of former New York Times media columnist David Carr that 'journalists are responsible for following the truth wherever it may guide them' (New York Times, 2013). While journalists may also be activists, Carr argues, 'activism can also impair vision'. He says: Activists can and often do reveal the truth, but the primary objective remains 'winning the argument' with the 'tendentiousness of ideology' creating 'its own argument' (New York Times, 2013).

The aim of this paper, though, is not to explore activism in its various forms and facets, but rather to shed light and provide focus on the impact of surveillance on democratic journalism through the contextualisation of journalists' practices and experiences.

Despite the reluctance with which many traditional journalists perceive any association with activism, a pillar of hope for a democratic fightback against surveillance rests on the emerging nexus between so-called hacker activists, or 'hacktivists', and journalists reporting on sensitive topics such as national security and mass surveillance, in which the hackers provide expertise on everything from online security involving encryption, to the actual provision to journalists of sensitive public interest information, and the journalists provide for the hackers a platform and reach that would be otherwise unattainable. This notion can be closely linked to a form of 'outsider journalism' beyond the confines and challenges of traditional journalism platforms. Such journalism may herald a form of 'sousveillance' of the future in the age of surveillance, particularly since there is a perception that traditional news platforms, facing an extraordinary array of challenges, including business model viability in the online age coupled with the explosion of public relations, influence exertion by corporate owners, the pressures of 24-hour live news environments, and now the surveillance-fuelled ability of governments to identify leaks and whistle-blowers – within or outside the confines of the law – are increasingly unable or unwilling to tackle all or any of the really sensitive stories about which it is crucial that citizenries in healthy democracies know.

Although journalists and hackers or hacktivists are in many respects fundamentally different, they share a similar platform in what Lyon (2015) calls the struggles over information freedom and control over information, and in some instances wear both hats at the same time. Examples include Julian Assange, and Jacob Appelbaum, a hacktivist who as a journalist collaborated with Der Spiegel on a number of articles covering the Snowden leaks. Appelbaum was also associated with WikiLeaks. Asked if we are seeing a move towards 'subversive' journalism bringing together outsider dissenting journalists and hacktivists, MacFadyen (interview, 16 March 2016) says 'without a doubt'. Former Guardian editor Rusbridger (interview, 25 April 2016) says: 'We've seen certain situations recently where journalists and hacktivists have collaborated. And we don't know where the recent Panama Papers come from but it looks at least possible that that came from a hack. Whenever we've worked with any of those kinds of people they are quite bemused by the lack of technical

knowledge or awareness that many of these (news) organisations have . . . we can learn from these people and should learn.'

In another example of such collaboration civil society NGOs are helping exiled Syrian journalists in Turkey use highly sophisticated security measures including encrypted software and protocols to minimise the potentially lethal likelihood that the Syrian or Turkish regimes, or jihadist groups, can infiltrate electronically. Amara worked with activists and IT specialists to travel to Syria undercover, to protect her online presence including social media accounts through VPN networks, installed in France. She gave a Syrian hacktivist control of her computer for four or five hours so he could install a VPN network that at that time was unbreakable by the Syrian authorities. She also mentioned as an example of effective citizen journalism in Syria the group of citizen journalists 'Raqqa is Being Slaughtered Silently', in reference to the IS-controlled northern Syrian city of Raqqa, who use the latest digital technology to gather and distribute information from the ground while circumventing surveillance by Islamic State. 'These guys are not professional journalists but they are taking so much risk . . . doing the same thing . . . and creating such an impact.' Meanwhile, US investigative news platform ProPublica has launched a version of its site on the dark web (through the anonymous Tor browser network), for readers who want to stay anonymous online (The Verge, 2016). Another example of the convergence of hacktivism and journalism is James Ball's transition from working for WikiLeaks to working on the Snowden leaks as a journalist for *The Guardian*. There are even joint hacktivism-investigative journalism conferences such as the CIJ Logan forum in Berlin, where a sense of common ground and goals prevails.

One of the challenges to this dynamic, however, is the fact that hacktivists do not enjoy the same protections as more easily identifiable journalists working for traditional media outlets. It recently emerged for, e.g. that Google was forced to secretly turn over a year's worth of Appelbaum's Gmail metadata – i.e. whom he emailed, when, and the details of IP addresses he used to log on to his Gmail account – to US investigators (The Intercept, 2015) as part of their investigation into WikiLeaks. Appelbaum has chosen to live in Berlin where, he says, 'the cost of physically harassing me or politically harassing me is much higher than when I last lived on U.S. soil' (The Intercept, 2015).

## Conclusions

An attempt of mutual watching, with the aim of bringing about transparency, lay at the core of the acquisition and dissemination of information in the WikiLeaks and Snowden affairs, and its transformation into journalistic material, in a continuation of a journalistic tradition that has understood itself as a watchdog. In this era of possible veillance, albeit it with an imbalance of scale and capacity tilted in favour of the State, journalism's attempt to take part in a 'normalised' veillance through the use of Big Data has severe implications that do not contribute towards more transparency, due to the imminent danger of watchdog journalism becoming unfeasible. We are finding journalists in a state of reacting to surveillance threats, within a climate of surveillance but not engaging unproblematically in surveillance themselves. If we accept that mutual watching is operationalised through whistleblowing, then the impact on journalism is problematic. Although journalism may have benefited from access to Big Data, it is also paying a high price.

As journalists, citizen journalists, and hacktivists converge in a form of new combined journalism seeking to challenge the Panoptic erosion of democracy, in defiance of the reluctance the media has traditionally displayed with regard to any affiliation with activism, or any notion of activist journalism, their task is facilitated by the same online digital world that has allowed for increased surveillance, but that also makes it easier for whistle-blowers to gather and transfer information to journalists.

However, throughout the world, the surveillance pushback against investigative and critical journalists pursuing sensitive stories, especially in the realm of national security and defence, is intense. The strategy of promoting submission and conformity through increasingly advanced and pervasive surveillance is a chilling thread that unites governments across the political spectrum, from superficially healthy democracies in danger of sliding into Panoptic homogenising self-censorship, eroded illiberal democracies riding waves of authoritarianism, populism and nationalism, and repressive regimes intent on retaining absolute power and control. In democracies, surveillance is not directly linked to the threat of assassination and torture, but its relentless march towards ever greater powers and ever fewer privacy safeguards, amid the establishment of favourable legislative and institutional governance parameters, is enough to chill the reporting climate and tilt the equiveillant balance of mutual veillance unmistakeably in favour of non-transparent state agencies. As democracy erodes more broadly, the pace of the shrinkage of watchdog journalism space picks up rapidly because the surveillance is increasingly unaccountable, aligns with politico-financial pressure, conducive new laws and a hollowed-out judiciary, and is linked to a broader array of veiled and direct threats, including imprisonment. Western democracies face the threat of an insidious surveillance-fuelled slide towards societal

submission and conformance that is a hallmark of undemocratic regimes.

Across the political spectrum surveillance tactics employed against journalists make demonstrative the power of the state while at the same time starkly underscoring the vulnerability of journalists' rights and protections. Apparently arbitrary decision-making on the surveillance of journalists may be designed to illustrate an intimidating power to disregard – in some instances even make – the 'rules' governing the flow of information in a society, and the fate of journalists. In Western countries, erosive legal frameworks often underpin the process. In repressive regimes the laws can be bent, interpreted and ignored at will. Ultimately, in both democratic and undemocratic countries the goal underlying the surveillance of journalists is the same: to cultivate a chilling effect that promotes conformance and submission to the dominant governing view. The only major difference lies is the degree of willingness and ability to resort to violence for those journalists who don't get the message. The current counter-tactics of journalists offer no guarantee as to future strategies. The cost of failure to stem the surveillance tide is incalculable in terms of personal resources, mental health and the future of democracy.

## Declaration of conflicting interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

## Funding

The author(s) received no financial support for the research, authorship, and/or publication of this article.

## References

Alwood E (2007) Watching the watchdogs: FBI spying on Journalists in the 1940s. *Journalism & Mass Communication Quarterly* 84(1): 137–150.

American Civil Liberties Union (2016) Surveillance under The Patriot Act. Available at: https://www.aclu.org/infographic/surveillance-under-patriot-act (accessed 29 April 2016).

Andrejevic M (2006) The discipline of watching: Detection, risk, and lateral surveillance. *Critical Studies in Media Communication* (23): 391–407.

Bakir V (2015) News, agenda building, and intelligence agencies. *The International Journal of Press/Politics* 20(2): 131–144.

Bakir V (2013) *Torture, Intelligence and Sousveillance in the War on Terror: Agenda-building Struggles*. Farnham, UK: Ashgate Publishing.

Bakir V (2010) *Sousveillance, Media and Strategic Political Communication: Iraq, USA, UK*. New York, NY: Continuum.

Bauman Z, Bigo D, Esteves P, et al. (2014) After Snowden: Rethinking the impact of surveillance. *International Political Sociology* 8(2): 121–144.

BBC (2014) Edward Snowden: Leaks that exposed US spy programme. Available at: http://www.bbc.com/news/world-us-canada-23123964 (accessed 29 April 2016).

Campbell JE and Carlson M (2002) Panopticon.com: Online surveillance and the commodification of privacy. *Journal of Broadcasting & Electronic Media* 46(4): 586–606.

Council of Europe (2015a) Resolution 2045 (2015) Mass surveillance. Available at: http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-EN.asp?fileid=21692&lang=en (accessed 22 July 2016).

Council of Europe (2015b) Nils Muižnieks: Democratic oversight of national security services in Europe remains "largely ineffective". Available at: http://www.humanrightseurope.org/2015/06/nils-muiznieks-democratic-oversight-of-national-security-services-in-europe-remains-largely-ineffective/ (accessed 14 July 2016).

Dover R and Goodman MS (eds) (2009) *Spinning Intelligence: Why Intelligence Needs the Media, Why the Media Needs Intelligence*. London, UK: C Hurst.

Electronic Frontier Foundation (2016) In hearing on Internet surveillance, nobody knows how many Americans impacted in data collection. Available at: https://www.eff.org/deeplinks/2016/05/hearing-internet-surveillance-nobody-knows-how-many-americans-impacted-data (accessed 15 July 2016).

Elmer G (2003) A diagram of panoptic surveillance. *New Media & Society* 5(2): 231–247.

Fernback J (2013) Sousveillance: Communities of resistance to the surveillance environment. *Telematics & Informatics* 30(1): 11–21.

Foreign Policy (2013) Metadata may not catch many terrorists but it's great at busting journalists' sources. Available at: http://foreignpolicy.com/2013/09/24/metadata-may-not-catch-many-terrorists-but-its-great-at-busting-journalists-sources/ (accessed 29 April 2016).

Freedom House (2016) Freedom of the press 2016. Available at: https://freedomhouse.org/report/freedom-press/freedom-press-2016 (accessed 29 April 2016).

Ganascia JG (2010) The generalized sousveillance society. *Special issue: Digitize and transfer* 49(3): 489–507.

Irish Times (2016): Sweeping surveillance powers planned by Dutch government. Available at: http://www.irishtimes.com/news/world/europe/sweeping-surveillance-powers-planned-by-dutch-government-1.2615109 (accessed 29 April 2016).

Lang GE and Lang K (1981) Watergate: An exploration of the agenda building process. In: Wilhoit GC and DeBock H (eds) *Mass Communication Review Yearbook*. Vol. 2, Beverly Hills, CA: Sage, pp. 447–468.

Lyon D (2015) *Surveillance after Snowden*. Cambridge, UK: Polity Press.

Lyon D (2003) *Surveillance after September 11*. Cambridge, UK: Polity Press.

Mann S and Ferenbok J (2013) New media and the power politics of sousveillance in a surveillance-dominated world. *Surveillance and Society* 11(1–2): 18–34.

Mann S, Fung J and Lo R (2006) Cyberglogging with camera phones: Steps towards equiveillance. In: *Multimedia: Proceedings of the 14th annual ACM international conference, (MULTIMEDIA '06)*, Santa Barbara, CA, USA, 23–27 October 2006, pp. 177–180.

Mann S, Nolan J and Wellman B (2003) Sousveillance: Inventing and using wearable computing devices for data collection in surveillance environments. *Surveillance & Society* 1(3): 331–355.

New York Times (2013) Journalism is still at work even when its practitioner has a slant. Available at: http://www.nytimes.com/2013/07/01/business/media/journalism-is-still-at-work-even-when-its-practitioner-has-a-slant.html?_r=0 (accessed 22 July 2016).

NiemanReports (2014) What's the difference between activism and journalism? Available at: http://niemanreports.org/articles/whats-the-difference-between-activism-and-journalism/ (accessed 22 July 2016).

onMedia (2014) Can journalists be activists? A conversation with Dan Gillmor. Available at: http://onmedia.dw-akademie.com/english/?p=19753 (accessed 22 July).

Re/code (2015) France has a powerful and controversial new surveillance law. Available at: http://recode.net/2015/11/14/france-has-a-powerful-and-controversial-new-surveillance-law/ (accessed 29 April 2016).

Reporters without Borders (2016) 2016 world press freedom index. Available at: https://rsf.org/en/ranking (accessed 29 April 2016).

Reuters (2013) Guardian says Britain forced it to destroy Snowden material. Available at: http://uk.reuters.com/article/uk-usa-security-snowden-guardian-idUKBRE97I10K20130820 (accessed 30 April 2016).

Reuters (2016a) Swedish prosecutors argue for upholding Assange arrest warrant. Available at: http://www.reuters.com/article/us-ecuador-sweden-assange-prosecutor-idUSKCN0XB0NU (accessed 29 April 2016).

Reuters (2016b) Snowden to take Norway to court to secure free passage. Available at: http://www.reuters.com/article/us-usa-security-snowden-norway-idUSKCN0XI1WU (accessed 29 April 2016).

Reuters (2016c) Poles rally against new surveillance law amid 'Orbanisation' fears. Available at: http://www.reuters.com/article/us-poland-protests-idUSKCN0V10JV (accessed 29 April 2016).

Spaulding S (2009) Off the blacklist, but still a target. *Journalism Studies* 10(6): 789–804.

The Guardian (2013) NSA files: Why the Guardian in London destroyed hard drives of leaked files. Available at: http://www.theguardian.com/world/2013/aug/20/nsa-snowden-files-drives-destroyed-london (accessed 30 April 2016).

The Guardian (2015a) GCHQ captured emails of journalists from top international media. Available at: http://www.theguardian.com/uk-news/2015/jan/19/gchq-intercepted-emails-journalists-ny-times-bbc-guardian-le-monde-reuters-nbc-washington-post (accessed 29 April 2016).

The Guardian (2015b) Chelsea Manning spends sixth Christmas in prison with no end in sight. Available at: http://www.theguardian.com/us-news/2015/dec/24/chelsea-manning-christmas-prison-whistleblower-wikileaks (accessed 29 April 2016).

The Guardian (2015c) Obama lawyers asked secret court to ignore public court's decision on spying. Available at: http://www.theguardian.com/world/2015/jun/09/obama-fisa-court-surveillance-phone-records (accessed 2 May 2016).

The Guardian (2015d) Spanish woman fined for posting picture of police parked in disabled bay. Available at: http://www.theguardian.com/world/2015/aug/16/spanish-woman-fined-gagging-law-photographing-police (accessed 29 April 2016).

The Guardian (2016a) LuxLeaks trial of tax whistle-blowers begins in Luxembourg. Available at: http://www.theguardian.com/world/2016/apr/26/luxleaks-trial-tax-whistle-blowers-begins-luxembourg (accessed 29 April 2016).

The Guardian (2016b) Labour demands more privacy safeguards in new surveillance laws. Available at: http://www.theguardian.com/world/2016/apr/04/labour-seeks-curbs-over-new-surveillance-law (accessed 29 April 2016).

The Intercept (2015) Revealed: How DOJ gagged Google over surveillance of Wikileaks volunteer. Available at: https://theintercept.com/2015/06/20/wikileaks-jacob-appelbaum-google-investigation/ (accessed 2 May 2016).

The Verge (2016) ProPublica is the first big news site optimized for the dark web. Available at: http://www.theverge.com/2016/1/8/10735518/propublica-dark-web-tor-hidden-service (accessed 2 May 2016).

White GL and Zimbardo PG (1980) The effects of threat of surveillance and actual surveillance on expressed opinions toward marijuana. *The Journal of Social Psychology* 111(1): 49–61.

This article is a part of Special theme on Veillance and Transparency. To see a full list of all articles in this special theme, please click here: http://bds.sagepub.com/content/veillance-and-transparency.